一学就会傻瓜书

超值彩色版

制作精美，杂志般的阅读享受
操作简单，一学就会的轻松体验

电脑安全与急救就这么简单

九州书源 曾福全 李显进◎编著



配超值多媒体光盘

"视频讲解+模拟操作"双重学习模式

与书中知识点一一对应，书盘结合

界面美观，配音标准，播放时长约12小时

赠送五笔查询小精灵软件和12000例电子书

清华大学出版社

一学就会傻瓜书

电脑安全与急救就这么简单

九州书源　曾福全　李显进◎编著

清华大学出版社
北　京

内 容 简 介

本书是一本帮助读者解决电脑安全问题的图书，主要内容包括认识电脑面临的各种威胁、黑客的攻击手段与防范方法、木马与病毒的特征与防范、如何限制他人使用电脑、通过各种手段打造安全的操作系统、使用防火墙加固电脑安全、电脑上网安全与防范、加密和解密文件、数据信息的备份和恢复、操作系统的备份和恢复以及典型电脑故障急救方法。

本书适用于对电脑有一定了解，喜欢研究电脑，对电脑及互联网的安全防范充满兴趣和好奇心的各类用户，包括在校学生、国家公务员、公司的电脑安全与维护人员等。

图书在版编目（CIP）数据

电脑安全与急救就这么简单/九州书源编著. —北京：清华大学出版社，2012.9
（一学就会傻瓜书）

ISBN 978-7-302-28154-2

I. ①电… II. ①九… III. ①电子计算机-安全技术 IV. ①TP309

中国版本图书馆CIP数据核字（2012）第034397号

责任编辑：朱英彪
封面设计：刘　超
版式设计：文森时代
责任校对：柴　燕
责任印制：
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：145mm×210mm　**印　　张**：9.125　**字　　数**：376千字
（附CD光盘1张）
版　　次：2012年9月第1版　**印　　次**：2012年9月第1次印刷
印　　数：1～6000
定　　价：32.80元

产品编号：044236-01



同样学电脑安全，为什么不让自己学得轻松点？
同样学电脑安全，为什么不学内容更全面的？
同样是安全与急救，为什么不选学以致用的？
同样是安全与急救，为什么不选可以随时查阅和学习的？

一个人每时每刻都会面临选择，而选择一本合适的参考书则是每个自学者最重要也最头痛的环节。“寓教于乐”是多年前就倡导的一种教育理念，但如何实现、以什么形式体现，却是大多数教育专家研究的课题。我们认为，“寓教于乐”不仅可以体现在教学方式上，也可以体现在教材上。为此，我们创作了这套书，不管是在教学形式上，还是在讲解方式和排版方式上，都进行了一定的探索和创新，希望正在阅读本书的您，能像看杂志一样在轻松愉悦的环境中学会电脑安全与急救。



本书的特点有哪些

情景教学，和娜娜一起进步：本书不仅讲解了与电脑安全与急救相关的各种知识，而且也是主人公娜娜的学习过程，相信娜娜在学习过程中的疑惑您也曾遇到过，不过娜娜最终在阿伟老师的指点下，走出了困境，相信通过本书的指导，您一定可以成为第二个“娜娜”。

贴近生活，知识安排以实用为目的：学习的目的是为了解决实际应用的难题，正因为您的需要，我们才安排了本书的各节知识。您可能遇到过他人随意进入电脑修改文件、电脑病毒老是喜欢光顾自己、电脑系统频频出问题、QQ密码被盗等电脑安全与急救问题，别着急，书中会根据您的需要，一一为您安排相应的解决对策。

理论与实战结合，方能授之于渔：在讲解电脑安全与急救知识时，采用理论与实战相结合的模式，首先以理论的形式让您了解到电脑存在的安全隐患，然后以步骤实战的形式告诉您如何采取应对措施，让电脑安全、稳定地运行。

🔒 **排版轻松，带来阅读杂志般的愉悦：**为了让您学得轻松，在内容的排版上，我们吸取了杂志的排版方式，样式灵活，不仅能满足视觉的需求，也能让您在充满美感的环境中学习到您需要的知识。



这本书适合哪些人

不管您年龄多大，现在正在干什么，如果您就是下面这些人中的他，拥有相同的困惑，就不妨拿起这本书翻翻，也许您将发现自己苦苦寻找的答案原来就在这不经意的字里行间。

正在上学的小A：小A和室友们都有电脑，还组成了局域网。虽然装了杀毒软件，但电脑还是经常感染病毒，于是，重装系统成为家常便饭，该怎么办呢？

在私企里充当“万金油”的小B：小B所在的公司正处于发展阶段，一般都是几个人共用一台电脑，可经常有人说文件丢失，这是完不成工作的借口还是确有其事？兼管公司硬件的小B纠结起来。

外资白领小C：小C在公司身居要位，每天会和各种文件打交道，而且很多都是公司机密，该怎么保证这些文件的安全呢？

小D、小E、小F……：他们都在使用电脑，却不能解决电脑出现的各种问题，特别是在当前这个黑客、木马、病毒泛滥的时代里，该如何做到安全使用电脑呢？

如果上面这些人都不是您，您只想通过这本书寻找攻击他人电脑、让他人电脑陷入瘫痪的方法，然后沾沾自喜，那这本书可能会让您失望。因为安全的电脑环境需要大家共同来维护，您可以了解攻击的方式，也可以了解侵入他人电脑的渠道，但谨记，这只是为了让您知道自己电脑和网络的弱点，加强防御而已。



有疑问可以找他们

本书由九州书源组织编写，参加本书编写、排版和校对的工作人员有曾福全、李显进、张良军、陈晓颖、简超、羊清忠、廖宵、向萍、王君、付琦、朱非、刘凡馨、李伟、范晶晶、任亚炫、赵云、陈良、张笑、余洪、常开忠、徐云江、陆小平、刘成林、杨明宇、杨颖、丛威、唐青、宋玉霞、刘可、何周和官小波。

如果您在学习的过程中遇到什么困难或疑惑，可以联系我们，我们会尽快为您解答，联系方式为QQ群：122144955，网址：http://www.jzbooks.com。

九州书源



目录

第01章　抨击电脑面临的威胁

1.1　来自外界的威胁........................2

1.1.1　黑客攻击........................2

1.1.2　病毒感染........................3

1.1.3　木马威胁........................5

1.2　电脑自身安全隐患........................7

1.2.1　电脑硬件的安全隐患..........7

1.2.2　操作系统的安全隐患..........10

1.2.3　个人信息的安全隐患..........11

1.2.4　网络信息安全问题..........13

1.3　更进一步——电脑安全技术........16

第 1 招　病毒防范技术..............16

第 2 招　修复系统漏洞..............16

第 3 招　充分利用防火墙..........17

第 4 招　访问控制技术..............17

第 5 招　为电脑设置权限..........18

第 6 招　备份与恢复数据..........18

1.4　活学活用........................18

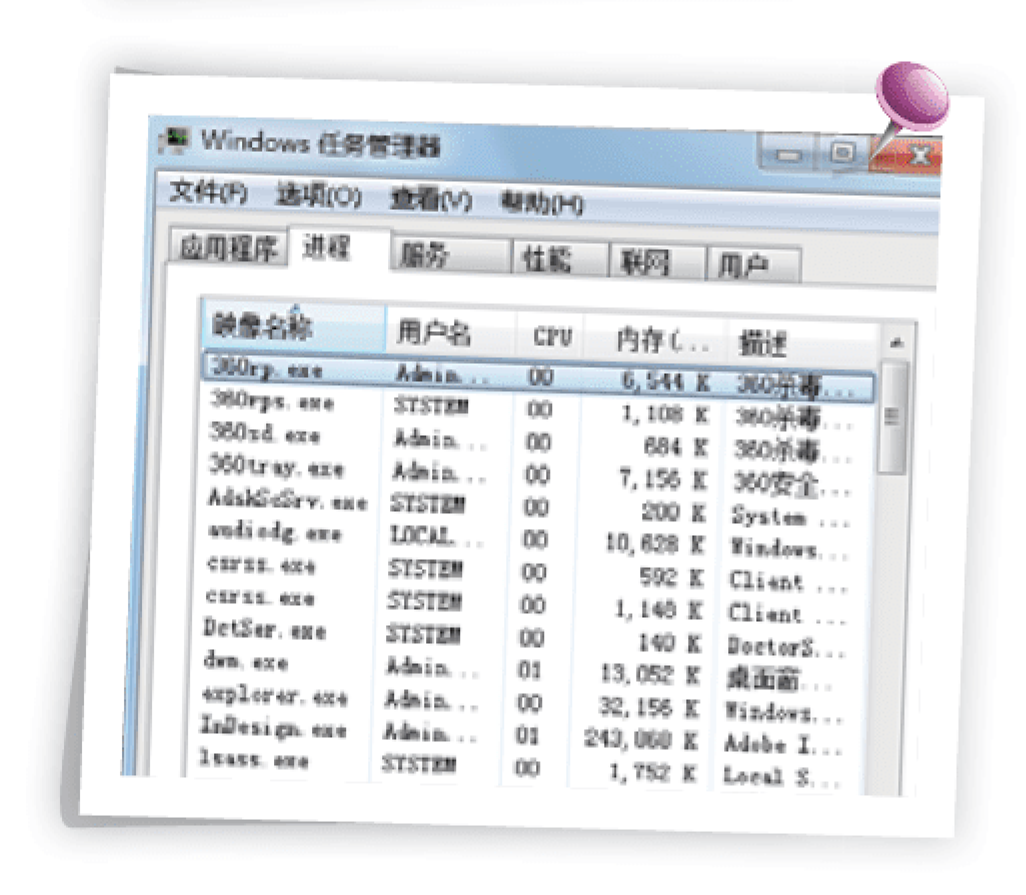
第02章　窥探黑客攻防的秘密

2.1　认识神秘的黑客........................22

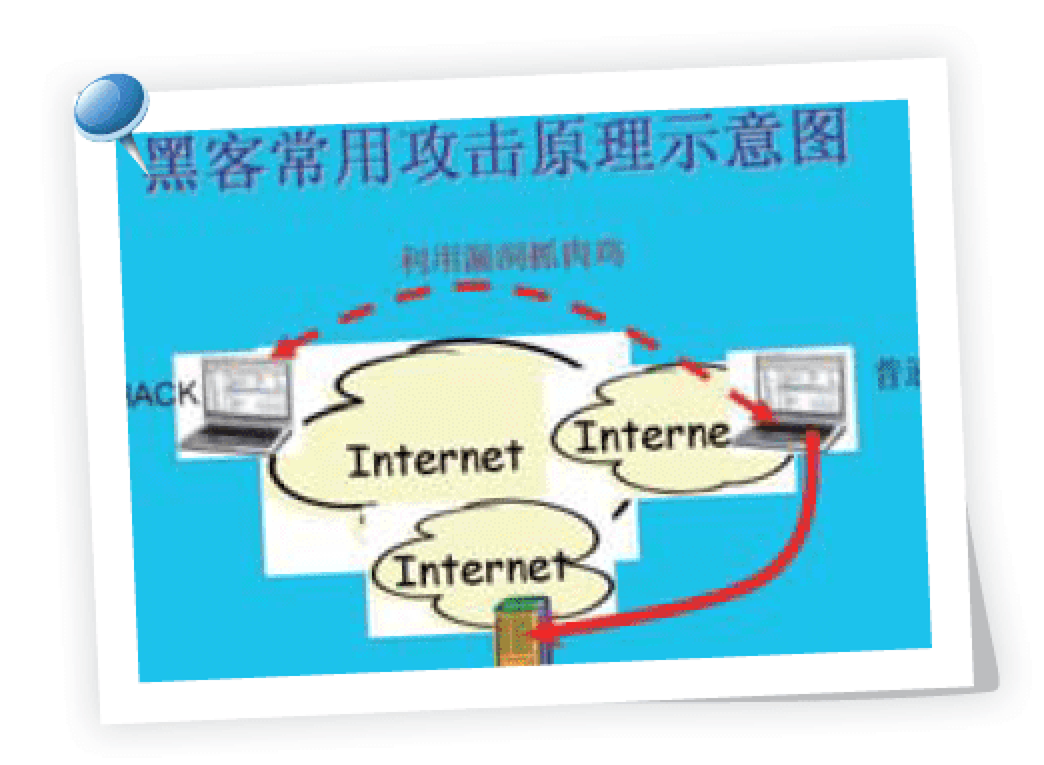
2.1.1　什么是黑客........................22

2.1.2　黑客攻击的目的和行为准则........................22

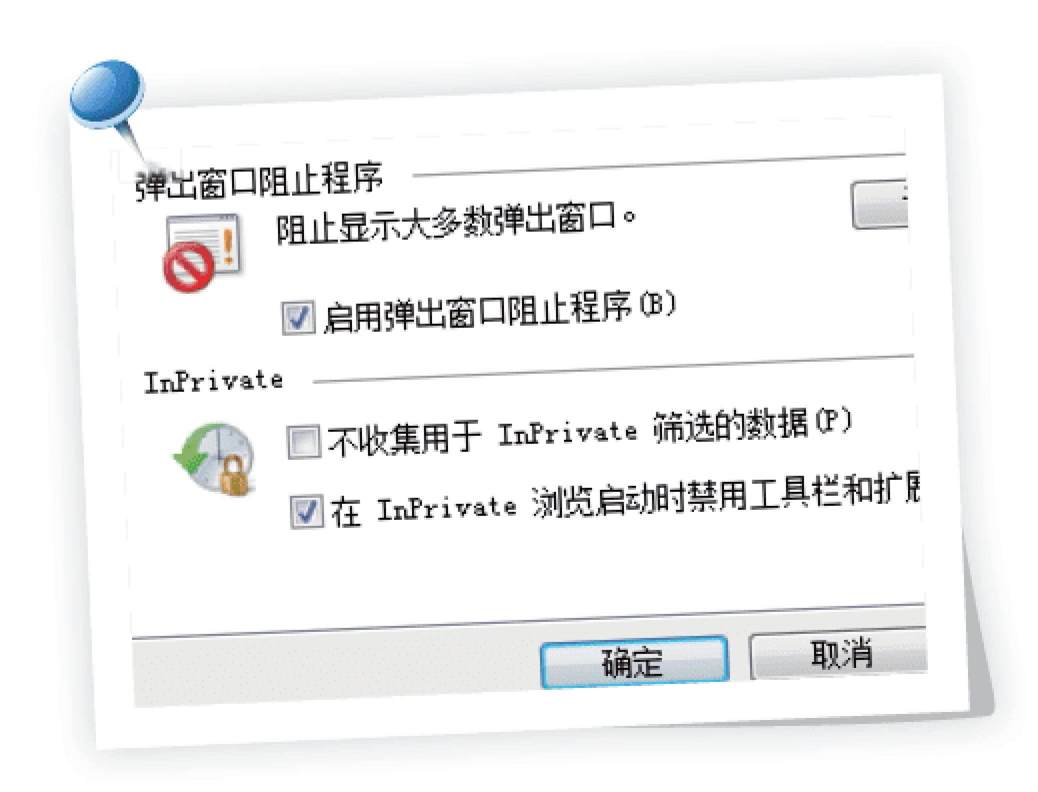
中文名	病毒名
网游盗号木马	Win32.Troj.OnlineGamesT
AUTO病毒	Win32.Troj.AutoRun
灰鸽子	Win32.Hack.Huigezi
熊猫烧香	Worm.WhBoy
AV终结者	Win32.Troj.AVKiller
艾妮	Win32.MyInfect













2.2　黑客攻击原理 24
2.3　常见黑客命令的使用 25
2.3.1　ping命令的使用 25
2.3.2　ipconfig命令的使用 26
2.3.3　net命令的使用 28
2.3.4　netstat命令的使用 28
2.3.5　tracert命令的使用 30
2.4　怎样防范黑客攻击 31
2.4.1　关闭端口 31
2.4.2　使用防火墙 33
2.4.3　隐藏IP地址 34
2.4.4　禁止ping命令探测电脑 35
2.4.5　减少用户账户 38
2.4.6　防止黑客破坏网上交易 39
2.5　更进一步——黑客常见攻击防范秘技 41
第 1 招　隐藏控制面板中指定项目 41
第 2 招　隐藏系统文件 41
第 3 招　设置IE阻止弹出窗口 42
第 4 招　关闭文件和打印共享 43
2.6　活学活用 43

第03章　拒绝病毒和木马的入侵

3.1　揭秘病毒和木马 46
3.1.1　病毒和木马的特征 46
3.1.2　如何发现病毒和木马 47
3.1.3　怎样预防病毒和木马 49
3.2　反病毒木马软件的应用 51
3.2.1　常见杀毒软件简介 51

3.2.2　360杀毒软件的应用 52
3.2.3　360木马防火墙的应用 54

3.3　遭遇新病毒该怎么办............56
3.3.1　对未知病毒的查找和分析 56
3.3.2　新型病毒处理 57
3.3.3　升级杀毒软件病毒库........59

3.4　更进一步——轻松处理病毒和木马............60
第 1 招　手动清除电脑病毒 60
第 2 招　使用QQ医生清除盗号木马 61
第 3 招　在安全模式下清除木马 61
第 4 招　设置注册表权限防御病毒和木马 62
第 5 招　清除端口木马 62

3.5　活学活用............63

第04章　限制他人使用电脑

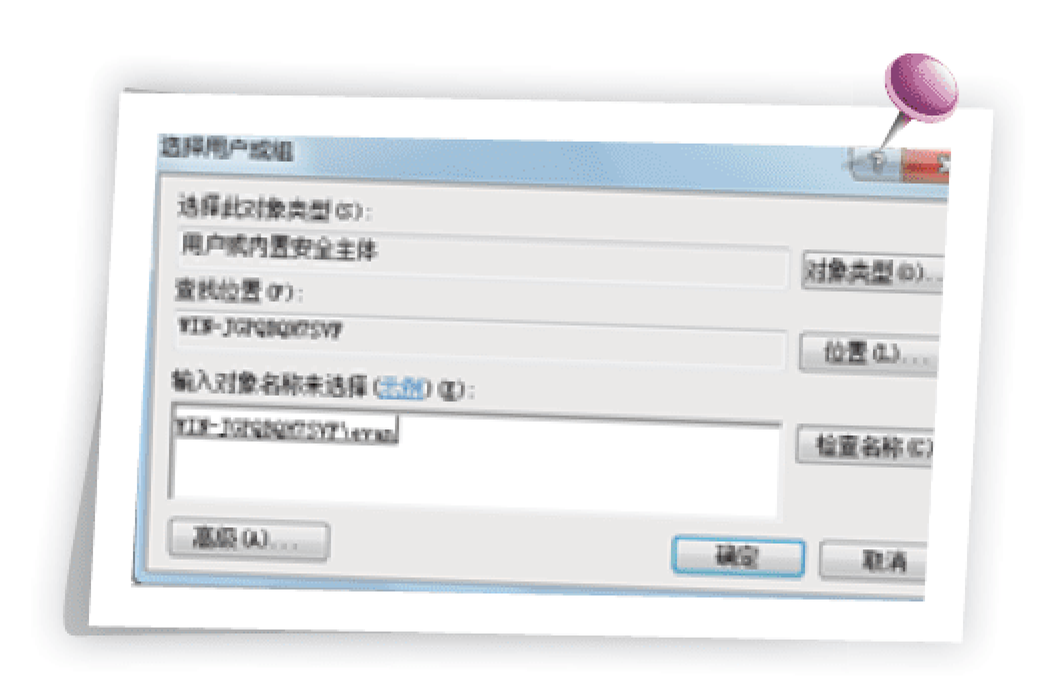
4.1　你的账户安全吗............66
4.1.1　重命名Administrator账户 ...66
4.1.2　禁用来宾账户 67
4.1.3　创建另一个管理员账户 69

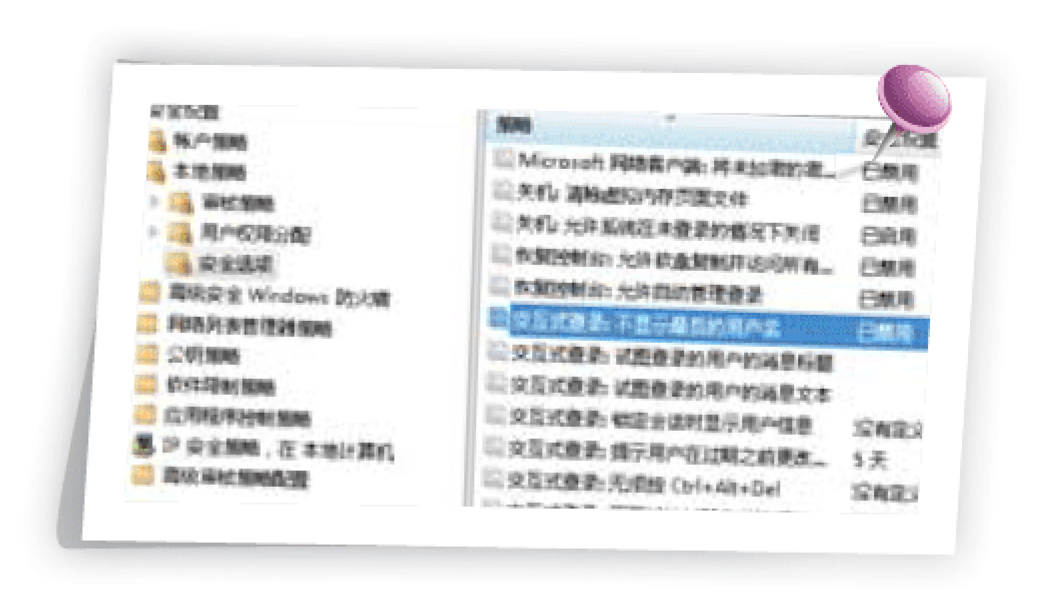
4.2　怎样安全登录电脑............71
4.2.1　在BIOS中设置登录密码.....72
4.2.2　锁定无效登录 73
4.2.3　不显示上一次登录名..........74
4.2.4　离开时锁定电脑..........75

4.3　设置用户权限 77

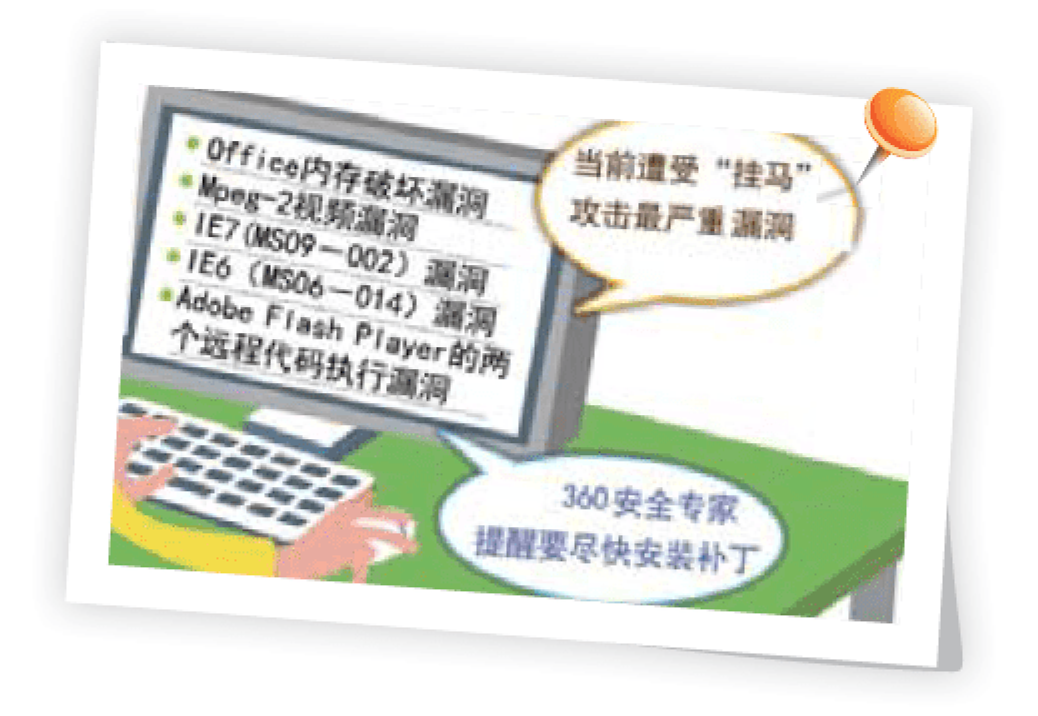






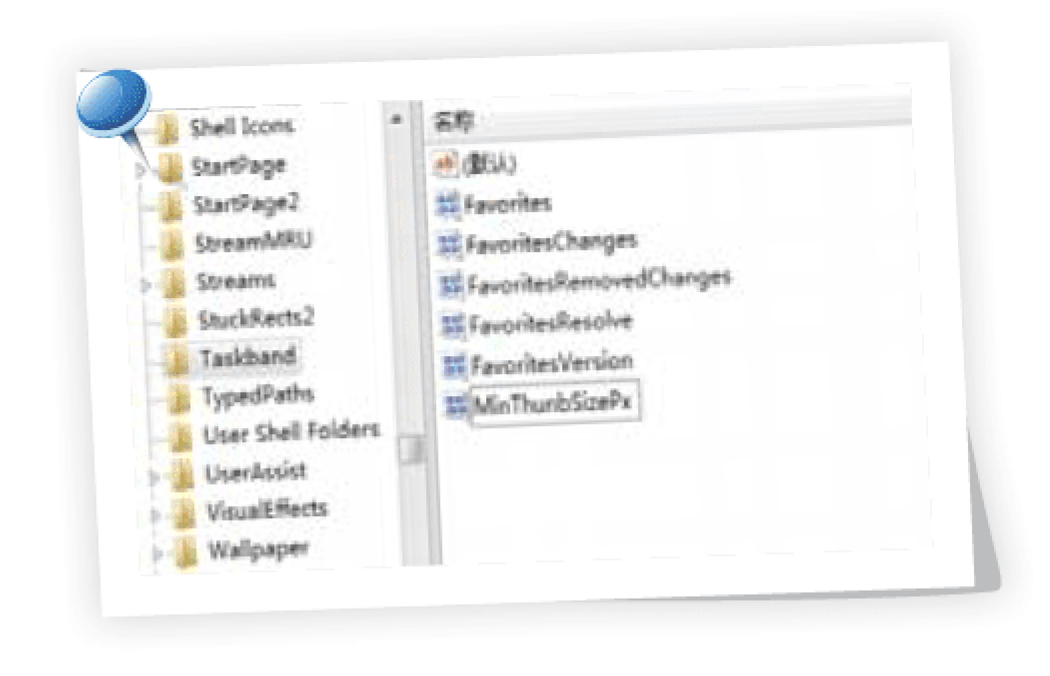


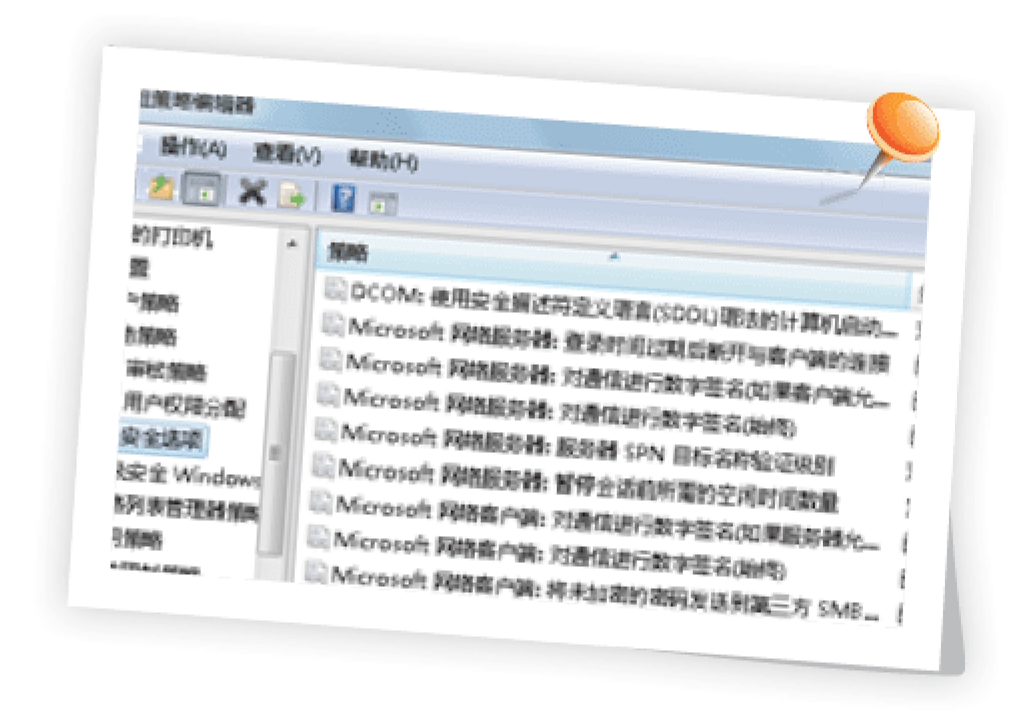
4.4 更进一步——限制他人使用电脑小秘招 79
第 1 招 设置账户的家长控制 80
第 2 招 登录系统桌面只显示背景图像 80
第 3 招 限制账户使用时间 81
4.5 活学活用 81



第05章 打造安全操作系统很简单

5.1 系统漏洞的修复 84
5.1.1 认识漏洞 84
5.1.2 新安装Windows系统中主要存在的漏洞 85
5.1.3 了解漏洞与系统攻击的关系 86
5.1.4 漏洞的分类 87
5.1.5 使用360安全卫士修复漏洞 88
5.2 系统组策略安全设置 90
5.2.1 认识组策略 90
5.2.2 禁止使用U盘 91
5.2.3 禁止更改桌面设置 92
5.2.4 禁止访问控制面板 93
5.3 注册表安全设置 94
5.3.1 认识注册表 94
5.3.2 备份和还原注册表 96
5.3.3 禁止危险的启动项 97
5.3.4 禁止远程修改注册表 98
5.3.5 禁止使用“开始”菜单 99
5.4 操作系统的其他安全技术 100







5.4.1　开启审核功能 101
5.4.2　检查日志........................102

5.5　更进一步——使用组策略和注册表小秘招 104

第 1 招　暂时隐藏不用的策略 105
第 2 招　将IE菜单栏移动到上方 105
第 3 招　调节Windows 7任务栏缩略图预览的大小......106

5.6　活学活用..................................106



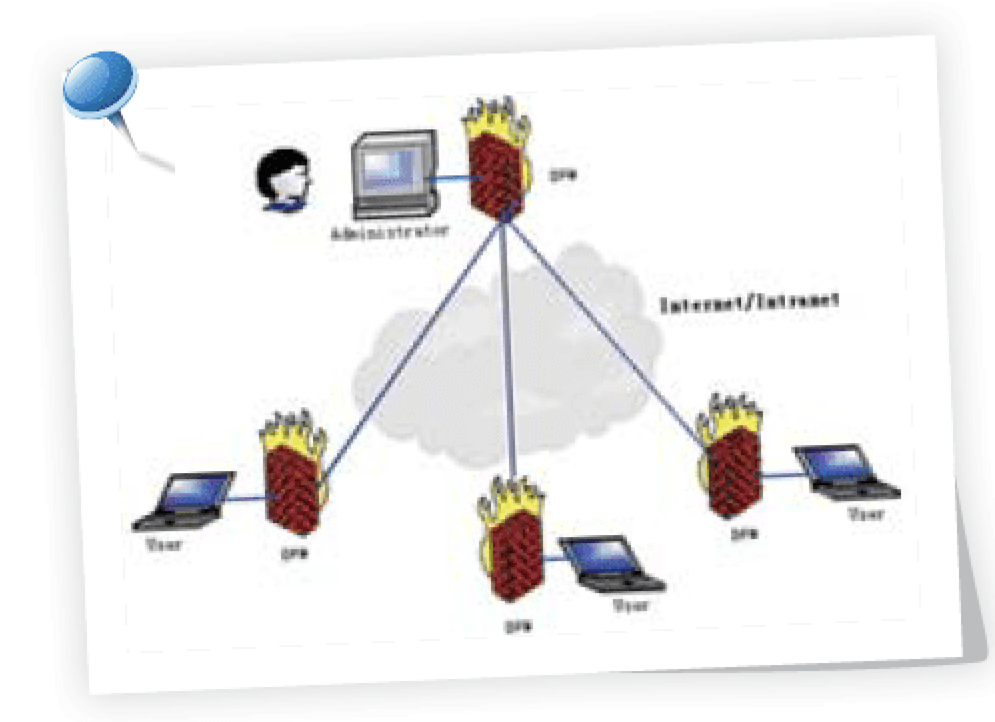


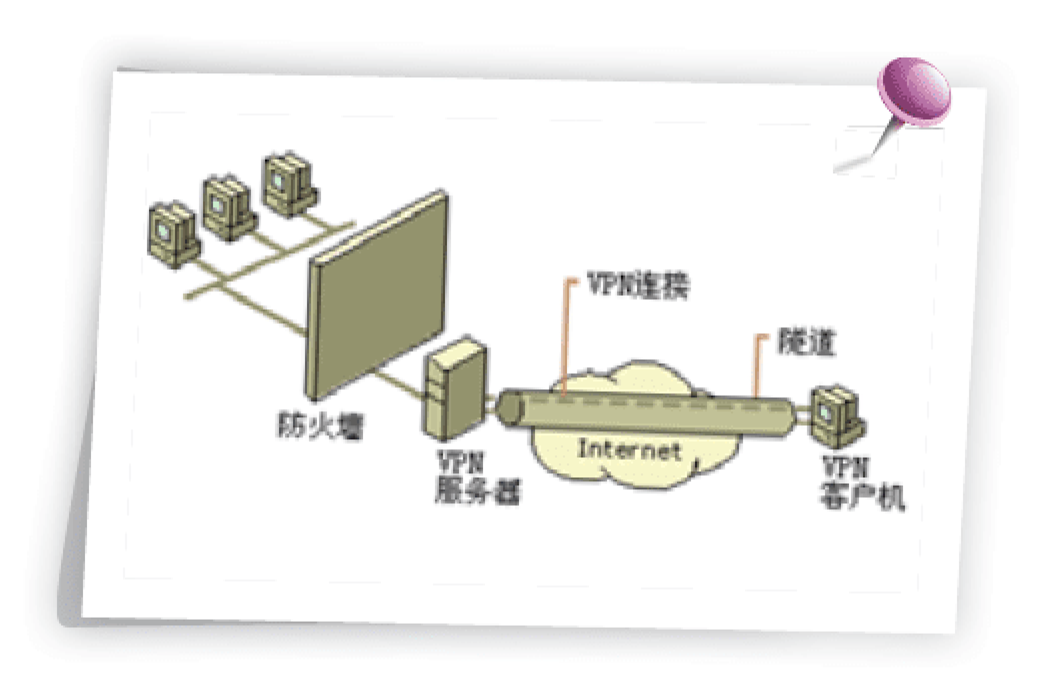
第06章　打造安全堡垒——防火墙

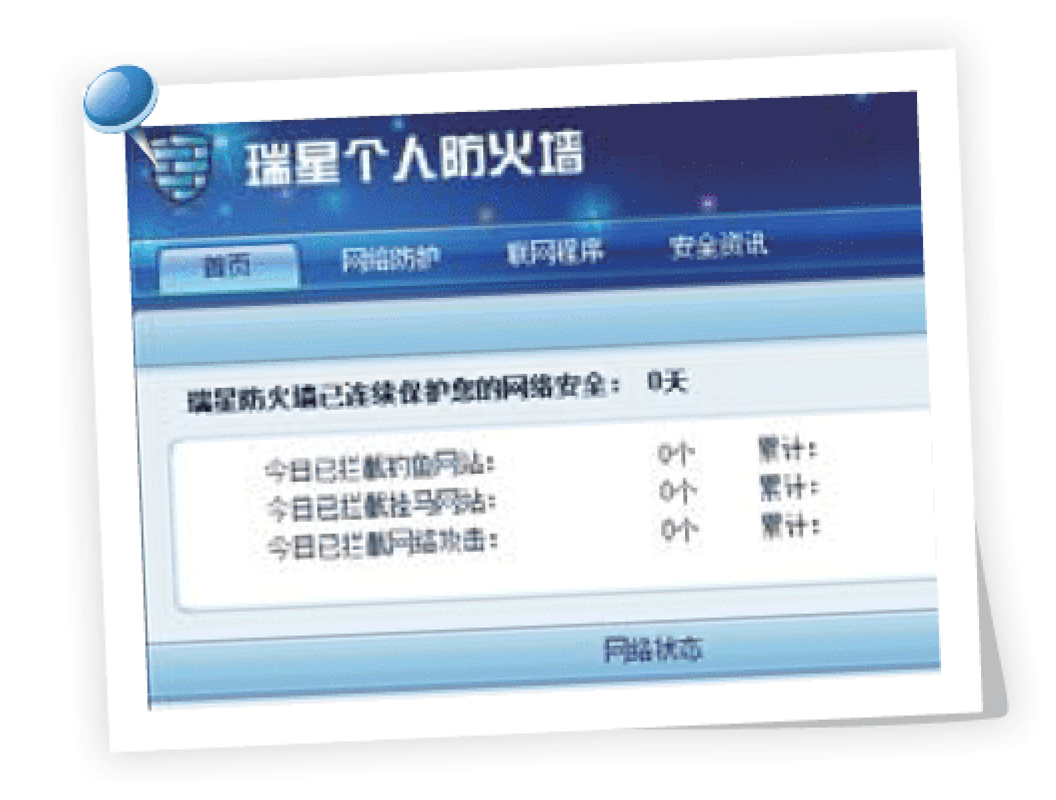
6.1　认识防火墙...............................108
6.1.1　什么是防火墙 108
6.1.2　防火墙的功能 108
6.1.3　个人电脑中使用的防火墙 109
6.1.4　防火墙的工作原理 110

6.2　Windows自带防火墙 111
6.2.1　启动系统自带的防火墙.... 111
6.2.2　设置允许的程序和功能....112
6.2.3　Windows 防火墙高级设置...113

6.3　网络防火墙...............................118
6.3.1　使用天网防火墙系统设置 118
6.3.2　设置应用程序规则 120
6.3.3　自定义IP规则..................121













6.3.4 使用瑞星防火墙 122

6.4 防火墙的选择 124

6.4.1 防火墙的种类 124

6.4.2 防火墙选择的误区 127

6.4.3 选择防火墙时需考虑的问题 128

6.4.4 个人防火墙的选择标准 129

6.5 更进一步——防火墙的秘密......130

第 1 招 创建FTP共享规则.......130

第 2 招 Windows 7防火墙的新程序提示 130

第 3 招 使用天网防火墙的设置向导 131

第 4 招 使用瑞星防火墙网络防护功能 131

6.6 活学活用............131

第07章 网络信息安全设置

7.1 设置Internet选项 134

7.1.1 设置Internet安全级别 134

7.1.2 设置可信站点 135

7.1.3 删除临时文件 136

7.2 使IE浏览器上网更安全 138

7.2.1 隐藏IE属性选项卡 138

7.2.2 禁用更改浏览器的主页 140

7.2.3 使用360安全卫士清除上网痕迹 142

7.3 安全使用电子邮件 144

7.3.1 过滤垃圾邮件 144

7.3.2 如何防御电子邮件炸弹....145

7.4 安全使用QQ....147

7.4.1 认识QQ漏洞....147

7.4.2 创建安全的QQ使用环境....148

7.5 网络安全防御....152

7.5.1 阻止恶意网络广告....152

7.5.2 阻止流氓软件入侵....154

7.6 更进一步——轻松保障网络信息安全....158

第 1 招 备份QQ聊天记录....158

第 2 招 清除IE历史记录....159

第 3 招 取消QQ即时状态....159

第 4 招 监控重要资料的访问行为....160

7.7 活学活用....160

第08章 给电脑加把锁——加密

8.1 密码的安全性....162

8.1.1 提高密码的安全性....162

8.1.2 保护密码安全的措施....165

8.1.3 常见密码泄露的现象....166

8.2 操作系统加密....168

8.2.1 设置登录密码....168

8.2.2 设置屏幕保护密码....168

8.2.3 设置电源管理密码....170

8.3 常见办公文档的加密....171

8.3.1 设置Word文档的密码....171

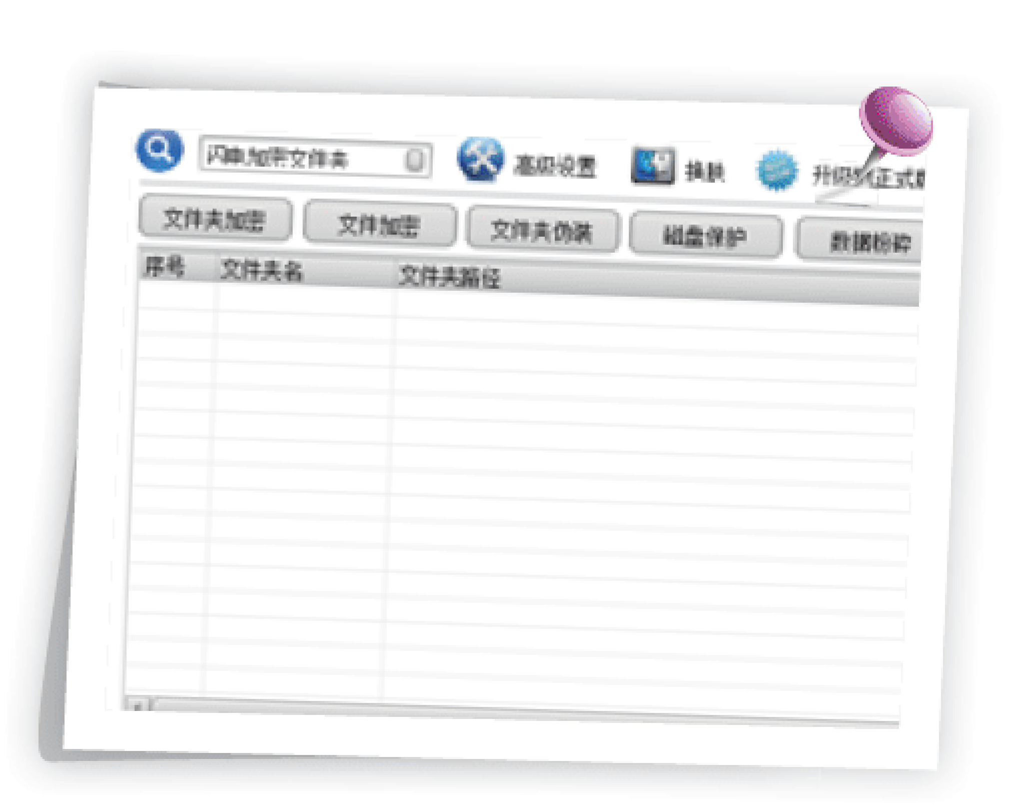
8.3.2 设置Excel文档的密码....172

8.3.3 设置Access数据库密码....174















8.4 文件及文件夹加密 176
- 8.4.1 文件及文件夹加密的方法 176
- 8.4.2 使用系统自带的加密功能进行加密 177
- 8.4.3 使用压缩软件加密文件和文件夹 181
- 8.4.4 使用文件夹加密超级大师加密文件 183

8.5 使用命令提示符创建安全文件夹 185

8.6 更进一步——轻松保护电脑安全 186
- 第 1 招 为电脑设置两个密码 ...186
- 第 2 招 设置密码后Windows 7也可以自动登录 187
- 第 3 招 隐藏Windows 7的“运行”命令 187

8.7 活学活用 188

第09章 数据备份防患于未然

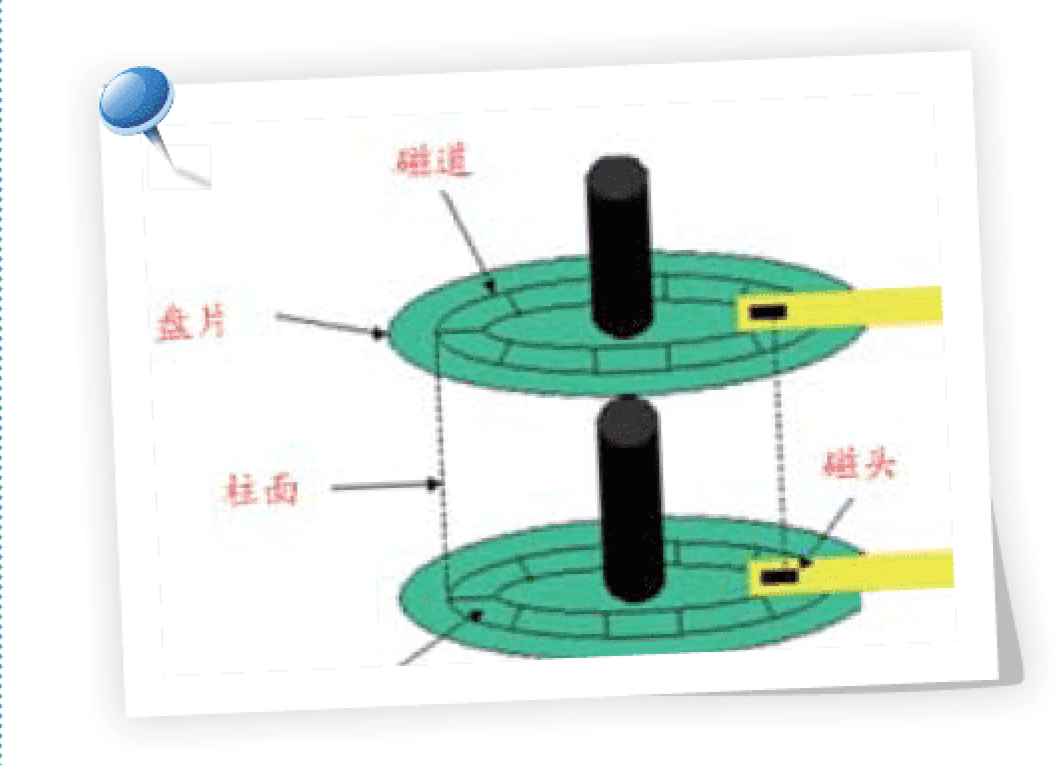
9.1 文件储存原理 190
- 9.1.1 硬盘存储数据的主要结构 190
- 9.1.2 文件的读取 192
- 9.1.3 文件的写入 193
- 9.1.4 文件的删除 193

9.2 恢复硬盘数据 194
- 9.2.1 硬盘数据恢复的范畴 194
- 9.2.2 使用FinalData恢复文件 ...194

9.2.3 使用360文件恢复功能恢复文件 197
9.2.4 其他的数据恢复软件........199
9.2.5 特殊情况下损坏数据的恢复....................201
9.3 备份和恢复重要数据...............202
9.3.1 备份和还原注册表 202
9.3.2 备份和还原驱动程序........205
9.3.3 备份和恢复文件 208
9.4 更进一步——硬盘数据小妙招 213
第 1 招 创建批处理文件备份注册表.....................214
第 2 招 不同系统中备份文件的访问................214
第 3 招 判断硬盘数据损坏原因...........................215
第 4 招 使用EasyRecovery简单恢复数据 215
第 5 招 驱动程序的手动备份...216
9.5 活学活用...................................216

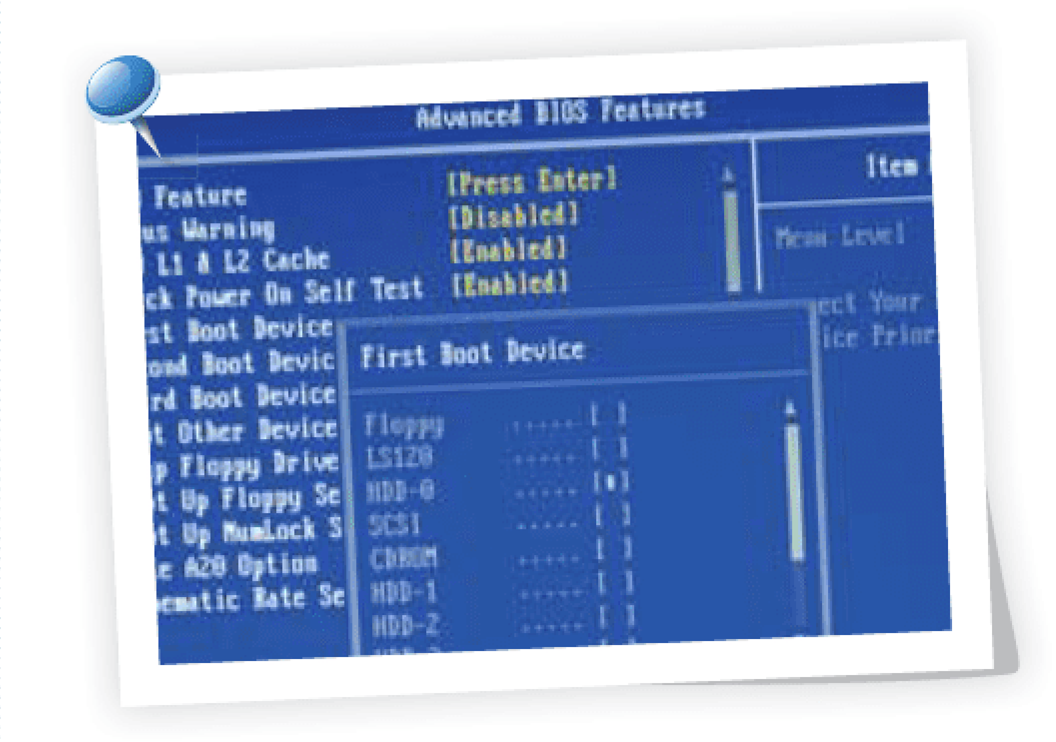
第10章 操作系统的急救

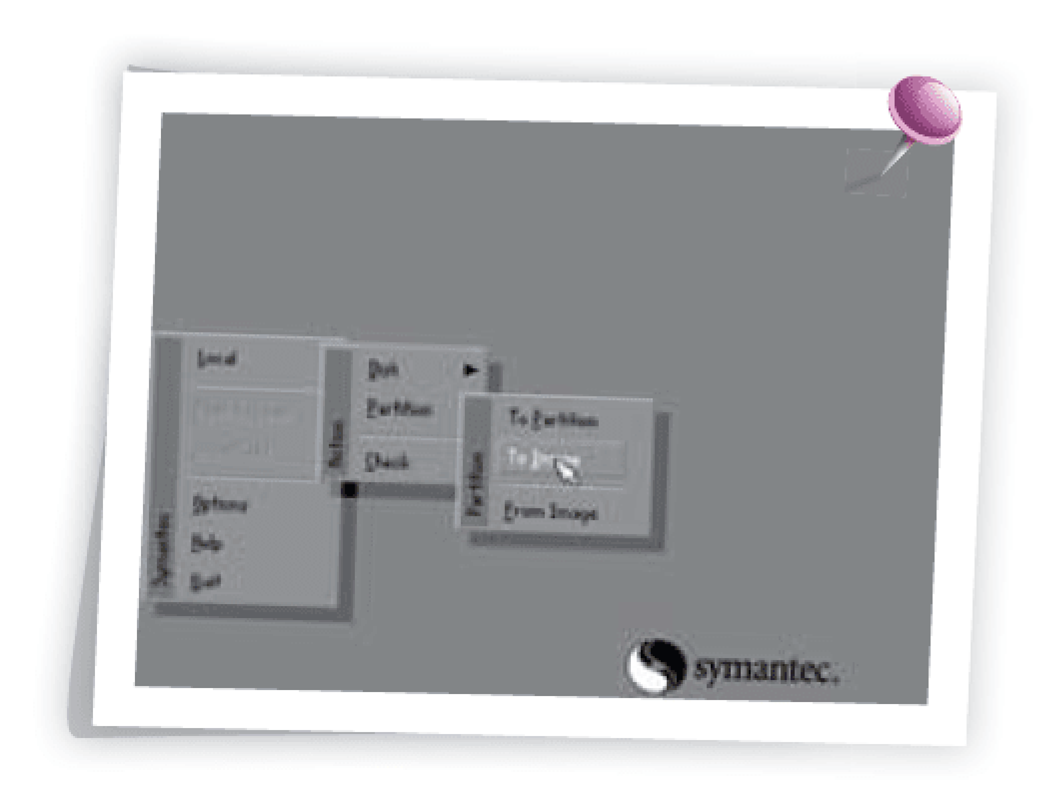
10.1 备份和还原操作系统...............218
10.1.1 使用MaxDOS软件备份操作系统 218
10.1.2 使用MaxDOS还原操作系统 222
10.2 重装操作系统 225
10.2.1 重装系统前的准备 225

















10.2.2 使用U盘启动重装 Windows 7......228
10.2.3 从光驱启动重装系统......233

10.3 使用系统还原点......235

10.3.1 创建系统还原点......235
10.3.2 通过还原点还原系统......237

10.4 恢复系统文件......239

10.5 更进一步——操作系统快速急救......241

第 1 招 恢复系统最后一次正确的配置......241
第 2 招 重注册DLL文件......242
第 3 招 注销当前用户......242
第 4 招 设置系统配置......243
第 5 招 设置Windows文件保护扫描......243

10.6 活学活用......244

第11章 典型电脑故障急救

11.1 操作系统自动重启......246

11.1.1 电脑自动重启的原因......246
11.1.2 电脑自动重启故障急救......250

11.2 电脑死机......252

11.2.1 电脑死机的原因......252
11.2.2 电脑死机故障急救......253

11.3 电脑蓝屏......255

11.3.1 电脑蓝屏的原因......256
11.3.2 蓝屏故障急救......257

11.4 IE浏览器故障急救......260

11.4.1 IE浏览器故障分析......260

11.4.2 IE浏览器故障急救实例 ...261

11.5 办公软件故障急救 266

11.5.1 Word故障急救 266

11.5.2 Excel故障急救 268

11.5.3 安装Office时出错 270

11.6 更进一步——故障轻松恢复 271

第 1 招 电脑开机时突然黑屏...271

第 2 招 IE浏览器提示出错并关闭网页 272

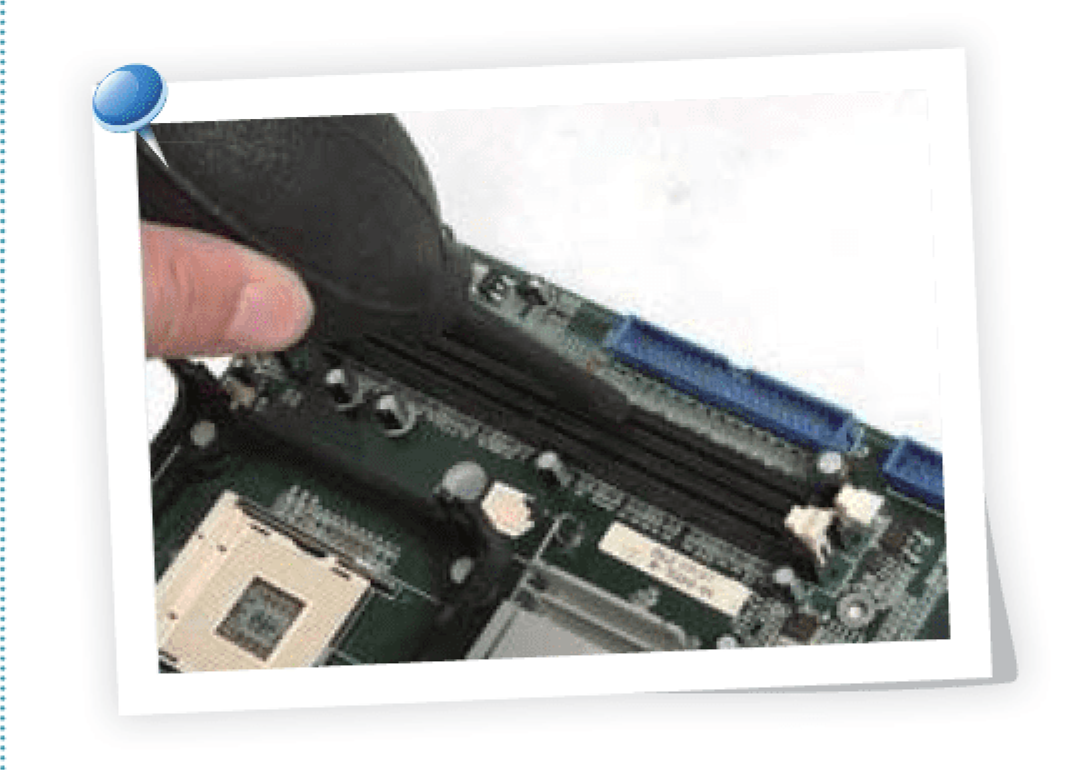
第 3 招 Windows 7开机后自动进入安全模式..............272

第 4 招 进行磁盘整理时反复重新开始..........................273

第 5 招 安装某些补丁时Explorer.exe出错 273

第 6 招 无法彻底删除Windows操作系统中的某些软件 274

11.7 活学活用 274







☑ 想知道你的电脑是怎样崩溃的吗？

☑ 怎样让电脑的硬件稳固工作呢？

☑ 电脑中的重要信息是怎样泄露出去的呢？

☑ 还在为电脑“偷懒”找不到原因而烦恼吗？



第 01 章

抨击电脑面临的威胁

今天，娜娜照常打开自己的电脑，但是刚进入桌面就不断地弹出对话框，提示“内存不足”，然后就死机。娜娜一下就傻了，不知道该怎么办才好。阿伟看见这种情况，对她说：“可能是电脑中病毒了，需要进入安全模式进行病毒查杀。”阿伟边操作边为娜娜讲解，最后将问题成功解决。娜娜觉得阿伟太厉害了，想让阿伟教她一些电脑安全方面的知识，于是对阿伟说：“阿伟，你得给我充一下电，以后我就能自己处理一些电脑的问题！”

1.1　来自外界的威胁

在为娜娜处理电脑问题时，阿伟告诉她：“电脑最常见的问题是来自外界的威胁，包括黑客的攻击、病毒和木马感染，它们无孔不入。因此，要提高电脑的安全性，首先应认识它们。”娜娜听了以后，迫切地要求阿伟逐一为她讲解这些知识。

1.1.1　黑客攻击

在计算机领域中，人们对黑客的态度褒贬不一。黑客的破坏性不容忽视，已经成为网络安全的克星，但也正因为黑客的存在，才促进了网络安全技术的不断发展。

新手解惑

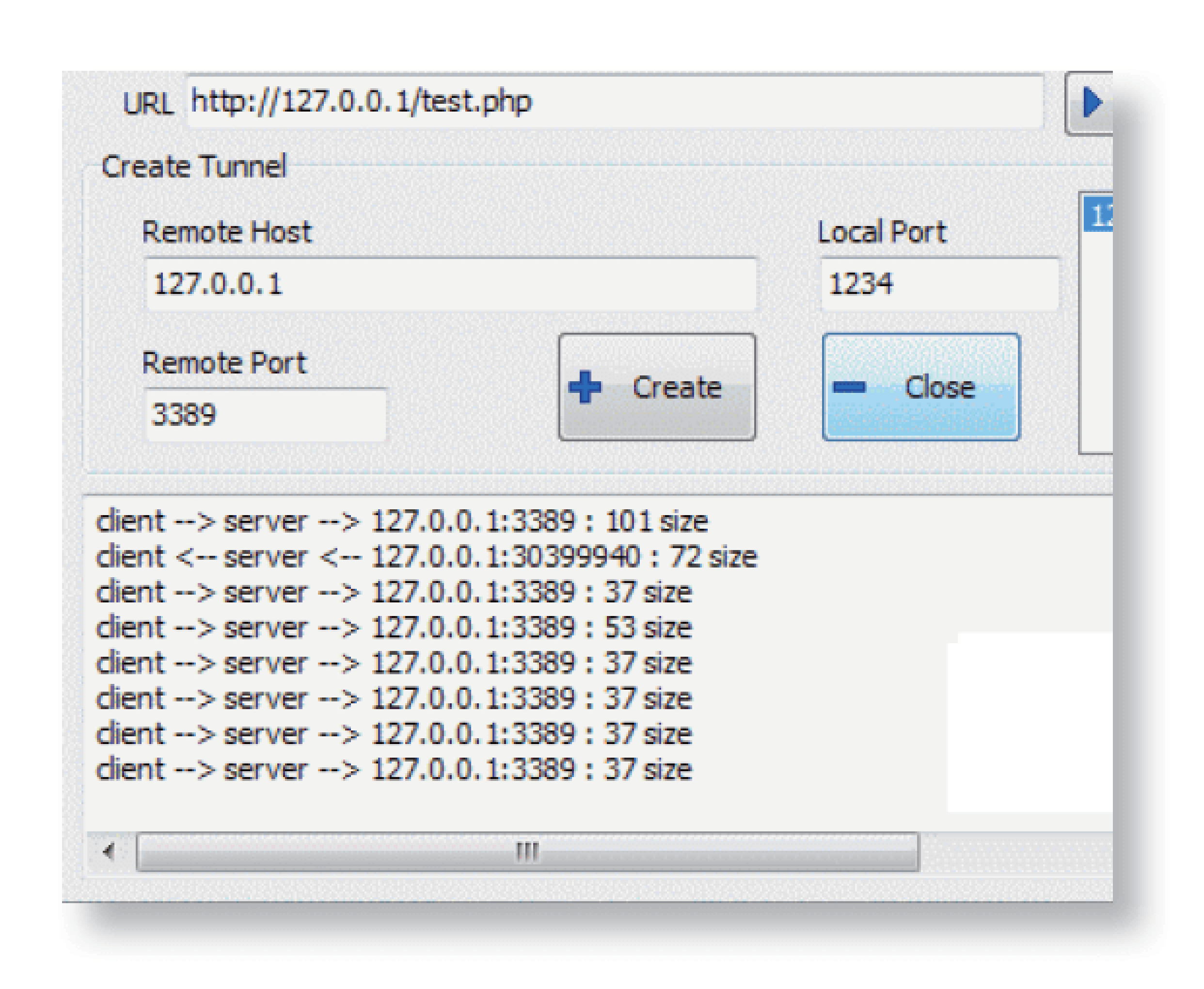


Q：黑客这个名字的来源是什么？

A：提起黑客，人们都觉得它很神秘。黑客可以是那些热衷于电脑技术并且水平高超的电脑专家，也可以是那些专门利用电脑网络搞破坏或恶作剧的家伙。黑客攻击电脑的主要目的是通过伪装自身，利用漏洞获取电脑信息或对电脑进行攻击。



黑客攻击的主要内容是什么呢？最常见的就是对网络端口进行监测以及通过漏洞和后门对网站进行攻击，下面将进行简单介绍。



1. 监测网络端口

网络端口是黑客主要的监测对象，它是电脑与外界通信交流的出口，因此，黑客可以利用监测所得的端口信息进行分析，确定攻击对象，达到破坏电脑的目的。

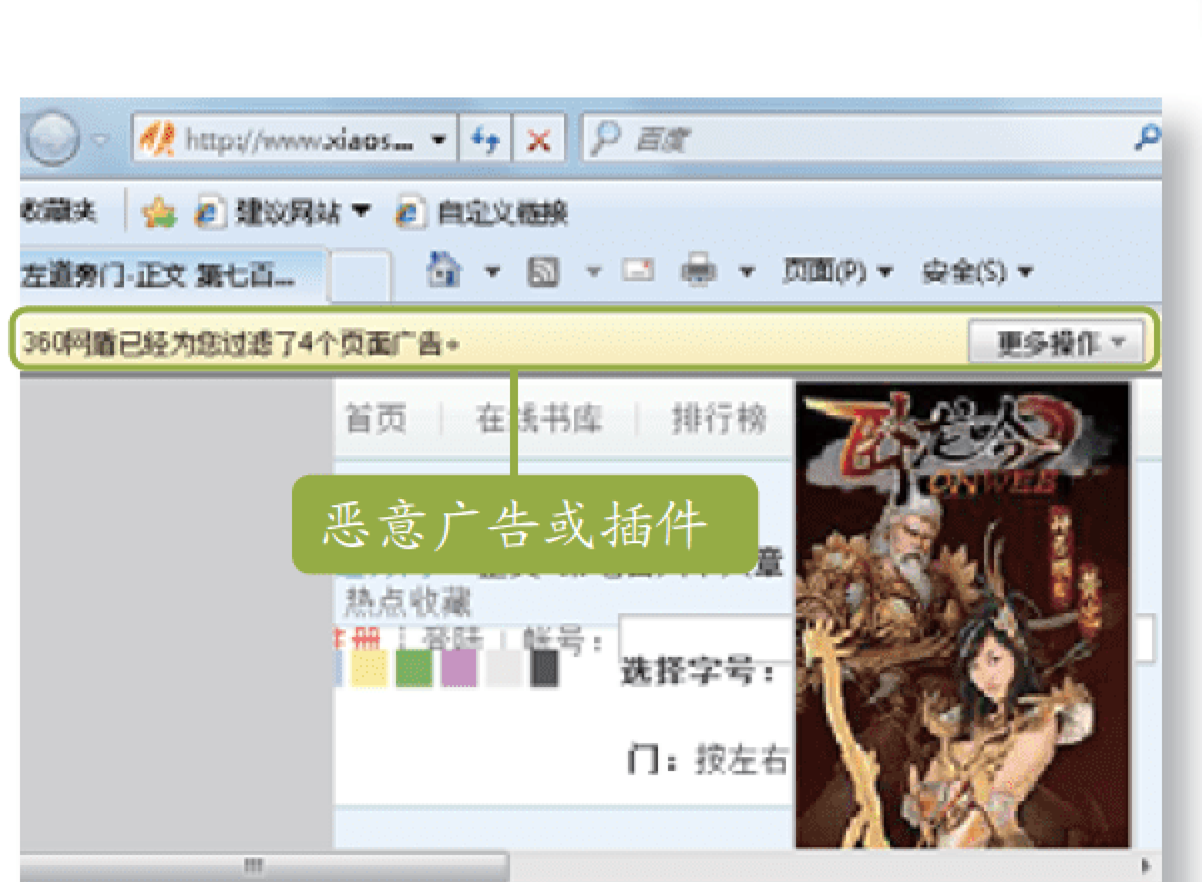


2. 攻击网站

黑客通过网页的漏洞，很容易得到网络管理员的账号和密码，甚至可得到一些网站权限设置不到位的服务器的最高权限，从而对网站进行入侵修改，以及信息获取。

黑客还可以利用一些人为因素进行攻击，即利用攻击目标的心理弱点来获取目标的信息。





3. 植入恶意广告和插件

浏览网页时，经常会有网站附带的插件或广告页面弹出，要求用户安装，甚至有时直接进行安装。这些广告和插件有可能是黑客植入进去的，会给用户带来极大的安全隐患。

1.1.2 病毒感染

很多人会感到疑惑，病毒到底是什么呢？一种专业的解释就是通过自身复制传播而产生破坏电脑功能或毁坏电脑数据的程序。其实，病毒就是作用在电脑中的一种病，它具有各种病状，也可通过“治病的良药”进行调理。



1. 病毒有哪些

电脑病毒的种类很多，主要分为引导型病毒、文件型病毒、蠕虫病毒、宏病毒和混合型病毒等。它们都具有各自的特征和感染对象。如近几年出现的一种著名病毒——熊猫烧香病毒，被感染的操作系统中所有.exe可执行文件全部被改成熊猫举着三根香的模样。



被熊猫烧香病毒感染后的文件图标

教你一招

防止电脑被黑客攻击和感染病毒的方法

在电脑中安装杀毒软件或安装防火墙能有效降低电脑被黑客攻击以及被病毒感染的频率，但因技术的发展和病毒的变异并不能完全阻止其威胁。

2. 判断电脑是否感染病毒

首先可以打开“任务管理器”，查看电脑中运行的进程，根据CPU和内存的占用率初步判断是否感染了病毒，其次可以查看CPU和内存的使用情况，确定电脑中是否存在病毒。

通常情况下，病毒会使CPU和内存的占用率提高，使其处于一个不正常的工作状态。

360Safe.exe	Administrator	00
360SE.exe	Administrator	11
ctfmon.exe	Administrator	00
360tray.exe	Administrator	00
conime.exe	Administrator	00
rundll32.exe	Administrator	00
safeboxTray.exe	Administrator	00
Explorer.EXE	Administrator	09
spoolsv.exe	SYSTEM	00
SOUNDMAN.EXE	Administrator	00
svchost.exe	LOCAL SERVICE	00
svchost.exe	NETWORK SERVICE	00

显示所有用户
这正常吗?
进程数：32 CPU 使用：100% 内存使用：

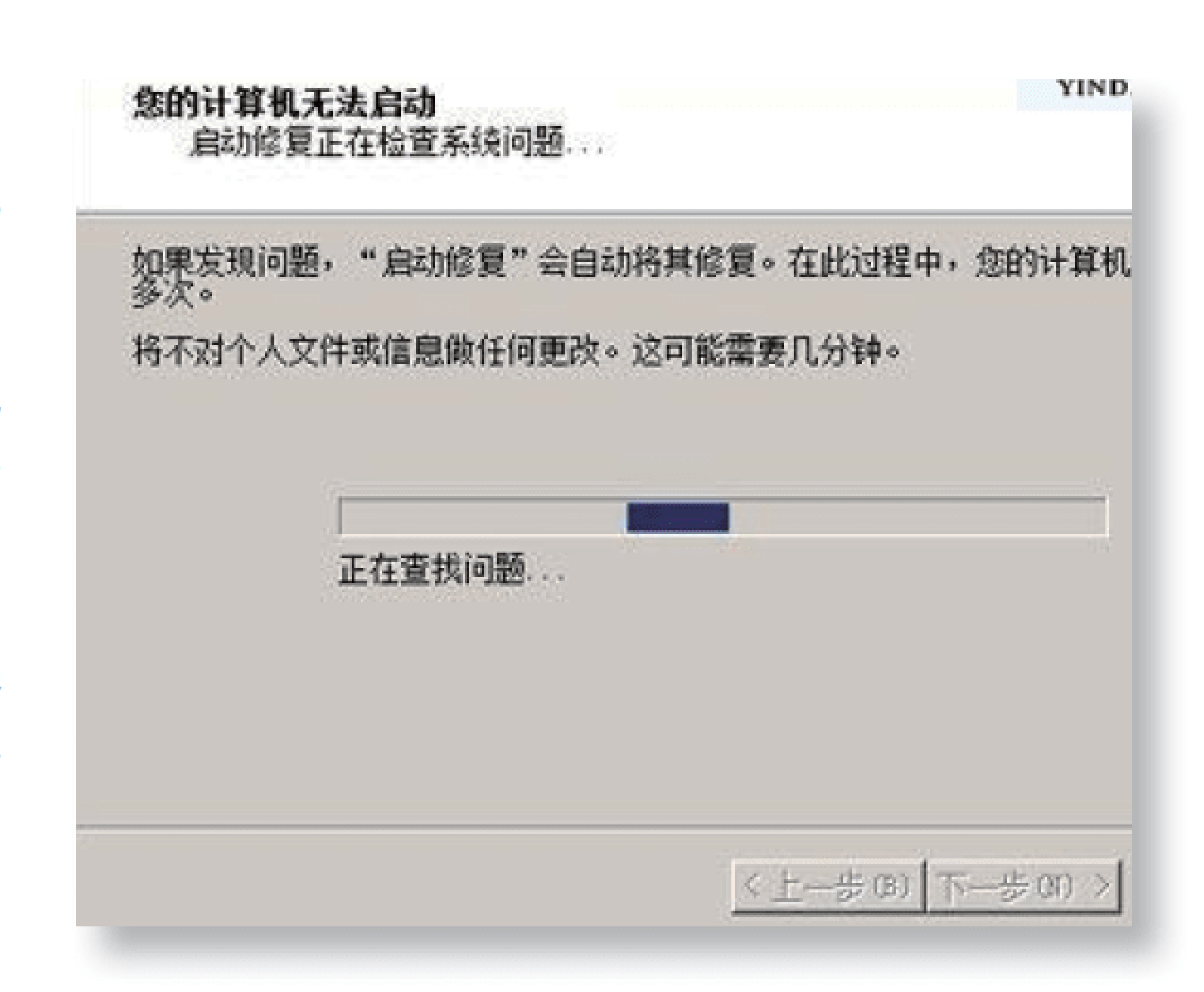
新手解惑

Q：病毒具有哪些特点？

A：病毒是通过自身复制传播而产生破坏电脑功能或毁坏数据作用的程序，一般寄生在系统引导扇区、设备驱动程序或者可执行文件内，并能够利用系统资源进行自我繁殖，从而破坏电脑系统。

3. 病毒导致系统文件丢失

系统文件丢失可能是由于病毒感染并破坏系统程序而导致的结果；卸载程序也可能导致系统文件丢失的现象，有的软件可能会共用一个系统文件，但被卸载后文件不见了，从而引起电脑频繁异常重启或者关机，当操作系统异常结束后，会对系统造成严重损伤。





教你一招

怎样判断系统文件是否丢失

大多数情况下，系统文件丢失都会弹出提示对话框，在其中将显示系统丢失的文件，通常表现为系统中相关功能或程序软件不可用。另外，系统文件丢失，也会造成系统无法启动等现象，具体应查看其错误提示。

1.1.3 木马威胁

木马程序是一种掩藏在美丽外表下打入电脑内部的东西。确切地说，它是一种经过伪装的欺骗性程序，即通过将自身伪装吸引用户下载执行，从而破坏或窃取使用者的重要文件和资料。



下面介绍木马的一些主要特征。

排名	中文名	病毒名
1	网游盗号木马	Win32.Troj.OnlineGamesT
2	AUTO病毒	Win32.Troj.AutoRun
3	灰鸽子	Win32.Hack.Huigezi
4	熊猫烧香	Worm.WhBoy
5	AV终结者	Win32.Troj.AVKiller
6	艾妮	Win32.MyInfect
7	MSN机器人	Worm.MSNBot
8	维金变种	Worm.Viking.gm

常见木马的排名

1. 木马的特点

木马程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开目标电脑的门户，使施种者可以任意毁坏、窃取目标电脑中的文件，甚至远程操控目标电脑。

2. 木马的启动方式

木马最常用的启动方式是通过注册表、win.ini、system.ini、某些特定程序或文件以及文件关联5种方式进行启动运行以控制并破坏电脑。



木马控制端

提示：通过注册表启动是最常用的木马启动方式，通过win.ini启动方式只被一些初级的木马设计者使用，木马程序在system.ini文件中加上其路径，也就可以保证永远随Windows启动，通过特定程序和文件启动方式又包括寄生于特定程序中与将特定的程序改名，文件关联启动方式是指木马程序会将自己与TXT文件或EXE文件关联。

新手解惑

Q：按木马的发展过程，可将其分为哪几个种类？

A：第一代木马：这一代木马功能简单，主要针对UNIX操作系统进行攻击，而针对Windows操作系统的木马则不多。该时期具有代表性的木马为BO、Netspy等。

第二代木马：这一代木马功能在大大加强，几乎能够进行所有的操作，且随着Internet的普及，开始通过网络进行大范围的传播。该时期具有代表性的木马主要有冰河与广外女生等。

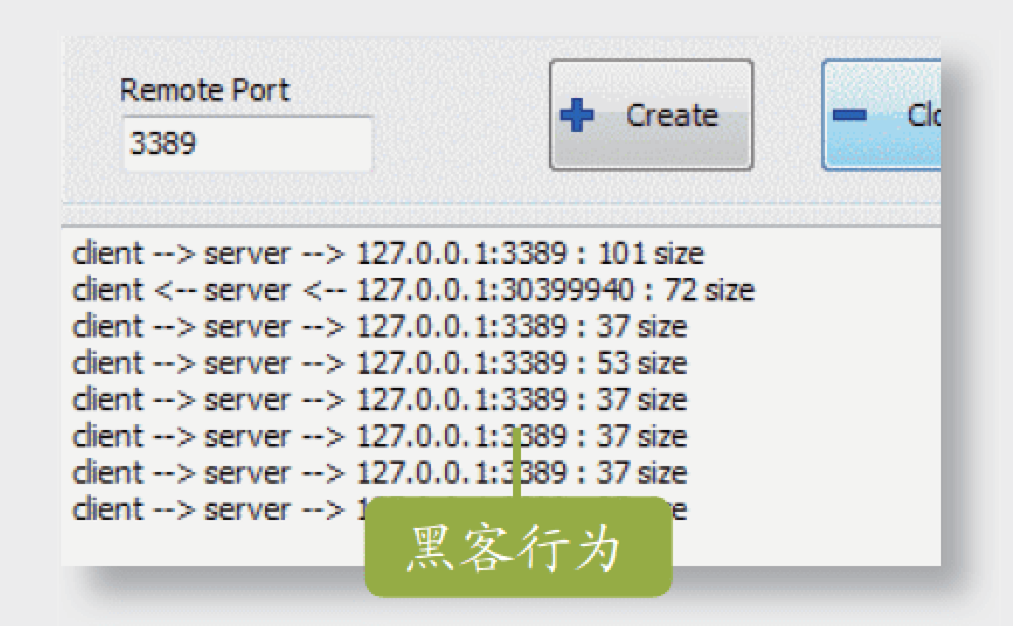
第三代木马：这一代木马继续完善连接与文件传输技术，除此之外，还增加了可以穿越防火墙的功能，并出现“反弹端口”技术，如灰鸽子等。

第四代木马：这一代木马除完善之前的所有技术外，还增加了进程隐藏技术，使被控端更难发现木马的存在，如广外幽灵与广外男生等。

跟我练习

认识并区别黑客、病毒和木马的特点

黑客利用监测所得的端口信息进行分析，确定攻击对象，达到破坏电脑的目的，并且黑客能利用病毒和木马来攻击电脑。病毒则是一种通过自身复制传播而产生破坏电脑功能或毁坏数据作用的程序。木马是一种经过伪装的欺骗性程序，通过将自身伪装吸引用户下载执行，以破坏或窃取对方的重要文件和资料。



ctfmon.exe	Administrator	00
360tray.exe	Administrator	00
conime.exe	Administrator	00
rundll32.exe	Administrator	00
safeboxTray.exe	Administrator	00
Explorer.EXE	Administrator	09
spoolsv.exe	SYSTEM	00
SOUNDMAN.EXE	Administrator	00
svchost.exe	LOCAL SERVICE	00
svchost.exe	SERVICE	00

病毒进程



1.2 电脑自身安全隐患

娜娜了解到黑客、病毒和木马对电脑的危害后又产生疑惑了，因为她以前遇到过很多造成电脑瘫痪的情况都与阿伟讲的不符，于是又问阿伟：“除了这些以外还有其他的原因会对电脑造成破坏吗？”阿伟告诉她：“当然还有，其实电脑自身的很多因素都会使其产生重大灾难，下面就给你详细讲解！”

1.2.1 电脑硬件的安全隐患

电脑硬件是影响电脑正常工作的主要因素，只有硬件稳固工作才能保证电脑的正常运行。



电脑硬件经常会因灰尘过多导致无法散热而产生电脑故障，或因天气的原因使其受潮等，因此灰尘和受潮等是影响电脑硬件安全的因素。但这些都能通过对其维护而得以解决。

1. 灰尘

定期为电脑的重要硬件或易被灰尘侵袭的硬件进行除尘也非常必要，可以延长其使用寿命。



将电脑放置于整洁的房间，并可套上防尘罩，避免灰尘太多对各电脑配件造成不良影响。





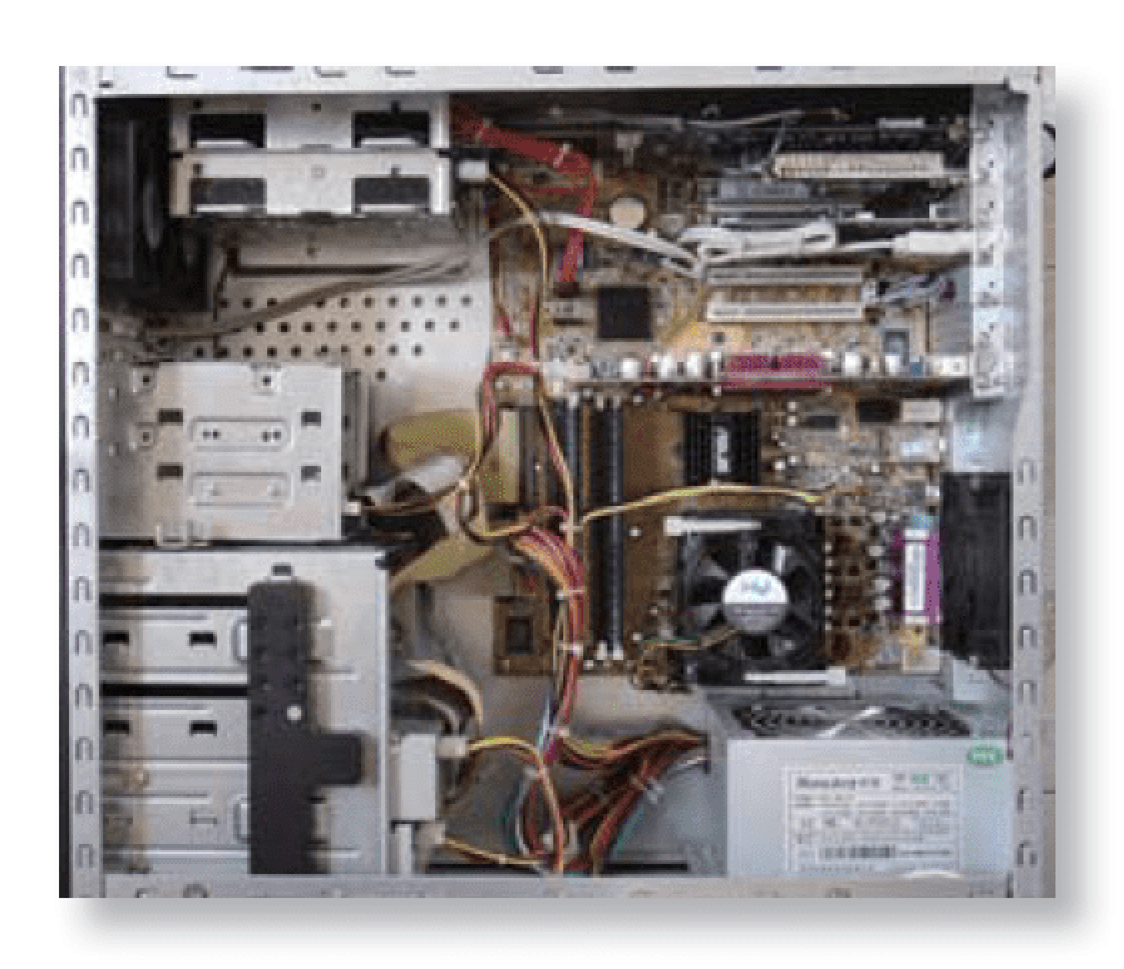
2. 受潮

电脑如果长期不使用，应该切断电源，但要定期开机运行一下，驱除其内的潮气，或将其重要部件喷上保护层以防止受潮 。

3. 电磁

电脑应该远离电场和磁场，通常电磁干扰来源于音响设备和大功率电器。较强的磁场不仅影响电脑的正常运行，甚至会使显示器出现抖动或花斑等现象，或使硬盘中的数据丢失或损坏。





4. 错误的使用

电脑各硬件组成电脑的硬件系统，电脑的运行是通过硬件的相互协作所支持的，如果电脑中的任意硬件设备使用不当，将会造成电脑的运行不正常，甚至会给电脑的其他硬件造成损坏。



5. 硬件自身质量问题

用户在选择电脑硬件时，通常会被市场上杂乱的品牌所迷惑，如不能很好地辨认其硬件好坏，很可能会购买到劣质的硬件设备，这些硬件本身存在着质量问题，因此，在使用过程中将存在较大的安全隐患。

教你一招

电脑硬件不兼容带来的安全隐患

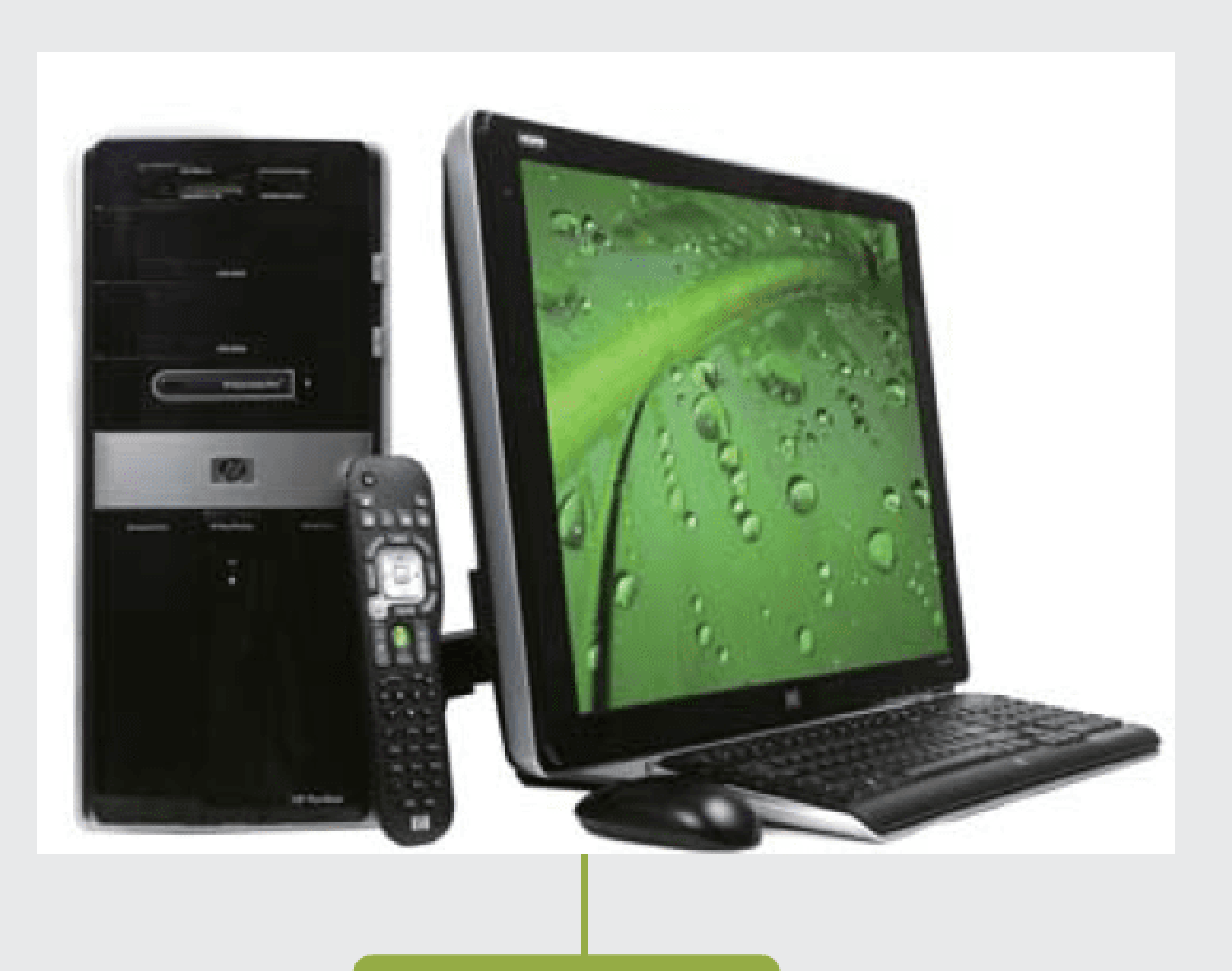
电脑的各种硬件都是由不同厂家生产和研发的，如主板的生产厂家有华硕、技嘉、微星以及精英等，即使各厂家之间尽量相互支持，但由于产品众多，且良莠不齐，因此，产品之间的兼容性问题在所难免。如用户电脑中的硬件兼容性存在问题，将会导致电脑使用不正常。



新手解惑

Q：影响电脑硬件正常工作的因素有哪些？

A：电脑硬件由众多元件组成，它是一个物理整体。影响电脑各硬件正常工作的因素主要有环境、电压与静电等，其具体内容介绍如下。



电脑的硬件系统

环境　温度范围：10~45℃，湿度范围：30%~80%

影响原因： 电脑的元件都非常精密，对所处的环境有一定的要求，其室内温度应保持在10～45℃之间，湿度范围最好在30%～80%之间，周围环境应洁净等。只有满足这些条件，才能使其正常工作，否则易引起元器件损坏，从而影响电脑的正常运行。

电压　电压范围：220V±10%，频率范围：50Hz±5%

影响原因： 电脑正常工作的电压范围为220V±10%，频率范围为50Hz±5%。日常所使用的电压经常发生波动，这种情况容易对电脑的电路与部件造成损害。

静电　防止静电

影响原因： 在安装或拆卸电脑时会产生静电，其对电脑硬件的危害最大，不仅会影响电脑部件的正常工作，严重时可能会击穿CPU、主板及内存等。

1.2.2 操作系统的安全隐患

操作系统是电脑运行的基本平台，也是文件操作和各种应用软件运行的场所，由于其结构相当复杂，其文件如果稍有差错将出现问题。



操作系统出现问题的主要原因包括其自身问题、进程管理、网络文件系统服务等，下面将分别进行讲解。

KB978632	Windows 7安全更新程序
KB981715	2007 Microsoft Office system 更新
KB980368	Windows系统安全更新程序
KB983484	Windows 7 更新程序
KB982300	Windows 7更新程序
KB2202188	Microsoft Office 2010 修补程序
KB2259539	Windows 7任务栏缩略图控制更新
KB2028560	Windows 7更新程序
KB2289116	Outlook Social Connector更新(32位)

1. 操作系统自身的问题

操作系统是一个庞大的软件系统，负责支撑应用程序的运行环境以及提供用户操作环境，同时也是电脑系统的核心与基石。它涉及了很多方面的应用，因此不可避免地存在一些缺陷（Bug）。黑客就是利用这些Bug作为攻击用户电脑系统的通道。

提示：操作系统的一些Bug可利用相关的软件进行修复，确保这些缺陷不被黑客等利用以危害系统安全。

2. 操作系统的进程管理

当创建的远程进程通过各种途径安装到电脑中时，用户将可以通过网络远程启动它们，从而使操作系统处于一个危险的环境中。

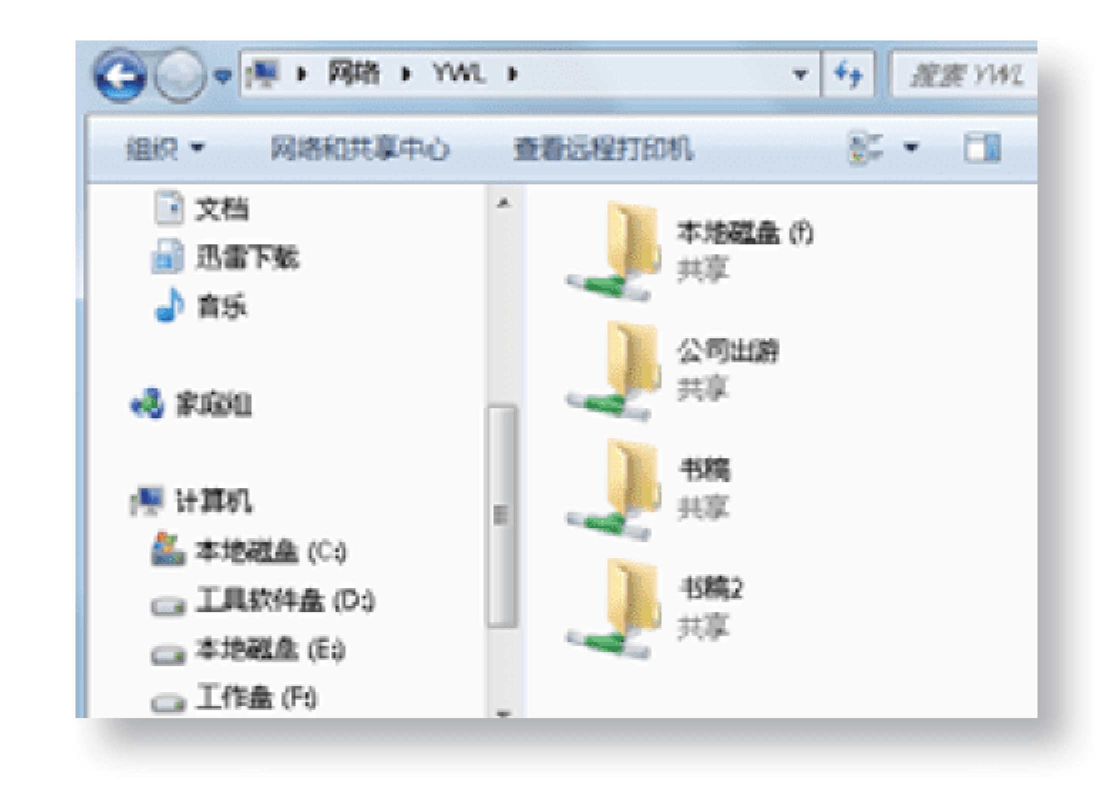


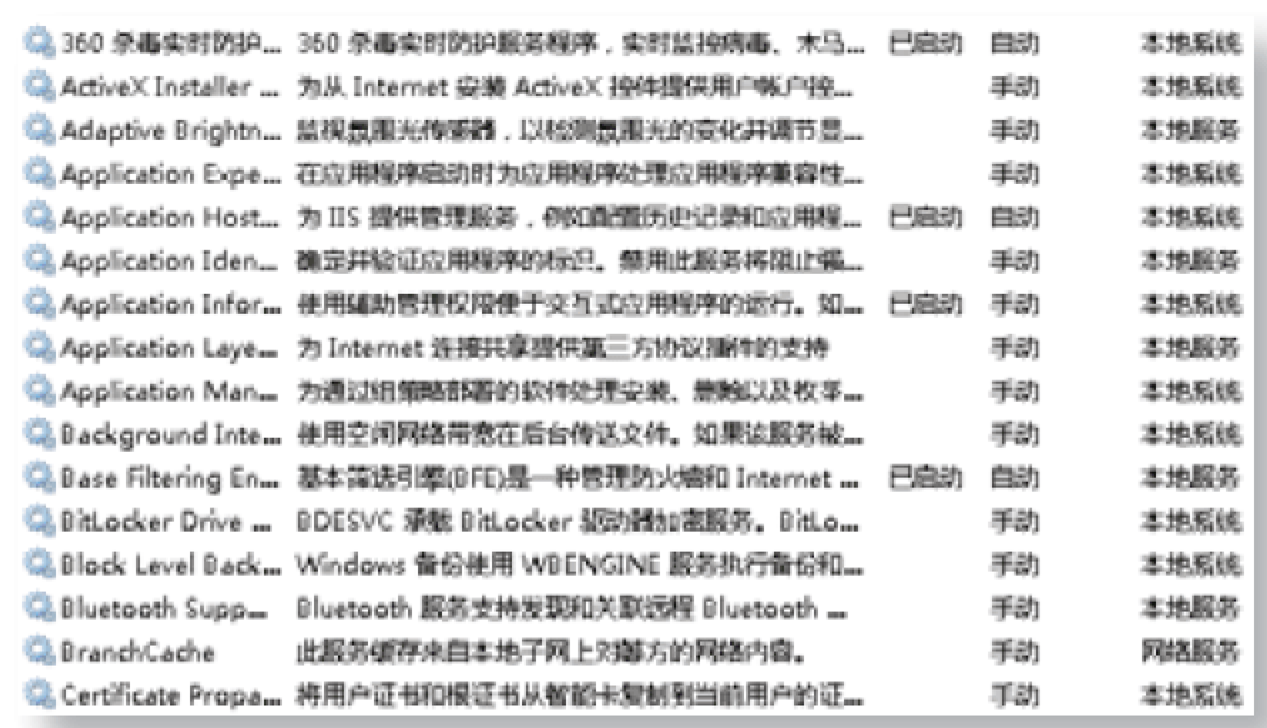
提示：在操作系统中，用户可以创建进程，甚至可以在网络上的其他电脑中创建并激活远程进程，而且所创建的远程进程将继承创建进程的某些权限。



3. 网络文件系统服务

用户在网络中的共享数据是通过操作系统中的文件系统服务得以实现的，操作系统为其提供的安全验证功能是有限的，因此，网络文件系统服务也是操作系统的一个重要的安全隐患。





360 杀毒实时防护...	360 杀毒实时防护服务程序，实时监控病毒、木马...	已启动	自动	本地系统
ActiveX Installer ...	为从 Internet 安装 ActiveX 控件提供用户帐户控...		手动	本地系统
Adaptive Brightn...	监视氛围光传感器，以检测氛围光的变化并调节显...		手动	本地服务
Application Expe...	在应用程序启动时为应用程序处理应用程序兼容性...		手动	本地系统
Application Host...	为 IIS 提供管理服务，例如配置历史记录和应用程...	已启动	自动	本地系统
Application Iden...	确定并验证应用程序的标识。禁用此服务将阻止强...		手动	本地服务
Application Infor...	使用辅助管理权限便于交互式应用程序的运行。如...	已启动	手动	本地系统
Application Laye...	为 Internet 连接共享提供第三方协议插件的支持		手动	本地服务
Application Man...	为通过组策略部署的软件处理安装、删除以及枚举...		手动	本地系统
Background Inte...	使用空闲网络带宽在后台传送文件。如果该服务被...		手动	本地系统
Base Filtering En...	基本筛选引擎(BFE)是一种管理防火墙和 Internet ...	已启动	自动	本地服务
BitLocker Drive ...	BDESVC 承载 BitLocker 驱动器加密服务。BitLo...		手动	本地系统
Block Level Back...	Windows 备份使用 WBENGINE 服务执行备份和...		手动	本地系统
Bluetooth Supp...	Bluetooth 服务支持发现和关联远程 Bluetooth ...		手动	本地服务
BranchCache	此服务缓存来自本地子网上对等方的网络内容。		手动	网络服务
Certificate Propa...	将用户证书和根证书从智能卡复制到当前用户的证...		手动	本地系统

4. 操作系统后门

操作系统后门是在操作系统的开发阶段，程序员常会在其中创建一些方便的后门，以便修改程序中的缺陷。如果后门被黑客探测到，或在操作系统发布之前未删除，那么它就成了安全隐患。



5. 操作系统自身的应用程序

操作系统具有自身的应用程序，通常这些应用程序也会存在威胁，如Adobe Flash以及IE浏览器，它们是操作系统中存在的最大威胁，很容易被黑客等利用，威胁电脑的安全。

1.2.3 个人信息的安全隐患

电脑中的个人信息除了各种应用程序、图形、文档、视频与音频等信息外，还包括账号和密码等信息，它们主要存储在电脑的硬盘、光盘、U盘或移动硬盘中，因此，当这些存储介质受到破坏时，其信息的安全将无法保证。



电脑的相关存储设备存在着许多与信息安全密切相关的特性，主要包括如下几方面。



问题1：存储过程中的损坏

损坏原因：当使用移动存储介质存储数据信息时，如果在存储的过程中意外中断或不正确退出，将有可能对资料造成破坏。

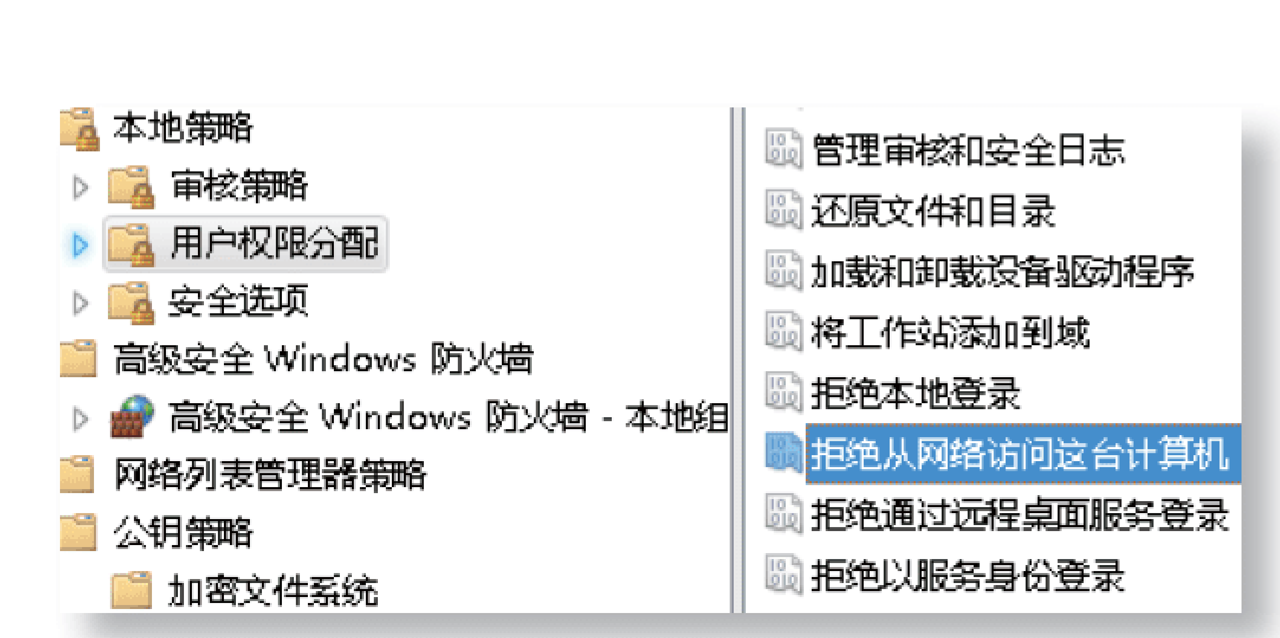
保证正确使用设备进行存储信息将有利于信息的安全存储。

提示：在电脑中，使用自身硬盘可以存储大量的信息，使用移动硬盘与U盘可以随身携带，在其存储或使用过程中很容易受到意外损坏，从而导致信息的损坏。

问题2：网络中用户对数据的访问

损坏原因：如果无任何权限设置，数据在网络中将被其他用户访问、更改，甚至破坏。

可在“本地安全策略”中设置拒绝从网络访问这台计算机，这样将有效保证数据的安全性。



提示：电脑中的数据可以很容易地被其他用户浏览或复制而不留痕迹，并且当网络中的用户获得访问个人数据的权限后，可以连接到存储信息的电脑中，并按其需要对信息进行复制或修改，甚至破坏。



问题3：黑客破坏数据的安全性

损坏原因：用户电脑中的信息可通过设置安全屏障以减少网络中各种不安全的访问，如开启系统的防火墙。

这种设置只对一般的使用者有效，对拥有高超的电脑技术的人或黑客则用处不大。



提示：用户在电脑中可以采用某些方法增加信息的安全性，但对于一些专业人员或黑客来说，将可能会越过这些屏障，破坏信息的安全，并且由于网络的发展，降低了信息的安全性。



问题4：个人用户密码的安全

损坏原因：用户在使用重要通信软件或网上银行时，对密码的设置应该谨慎，需要使用相对复杂的密码。

如用户使用的QQ软件，若账号密码丢失将使个人的聊天记录泄露，用户应通过对其设置密码保护等方式保护密码的安全。

教你一招

如何保护个人信息的安全

除将重要数据备份外，用户还可以将其加密并设置访问权限，防止他人对其进行破坏。

1.2.4 网络信息安全问题

随着Internet技术的发展，电脑中的信息都可在网络中共享。电脑网络信息的共享虽然给人们带来了极大的便利，但也将受到某些不安全因素的影响，从而出现安全问题，下面将分别对其进行讲解。



网络信息的安全问题包括网络管理员安全配置不当、用户安全意识不强等用户自身疏忽而造成的安全漏洞；或利用网络中信息的共享性而在用户电脑中种植木马；某些不法人员利用软件对电脑网络进行攻击，或传播非法信息等。



1. 管理员安全配置不当

用户在为电脑进行管理员安全配置时，如果对其安全属性配置过低，则很容易被网络中的木马程序盗取账户和密码。

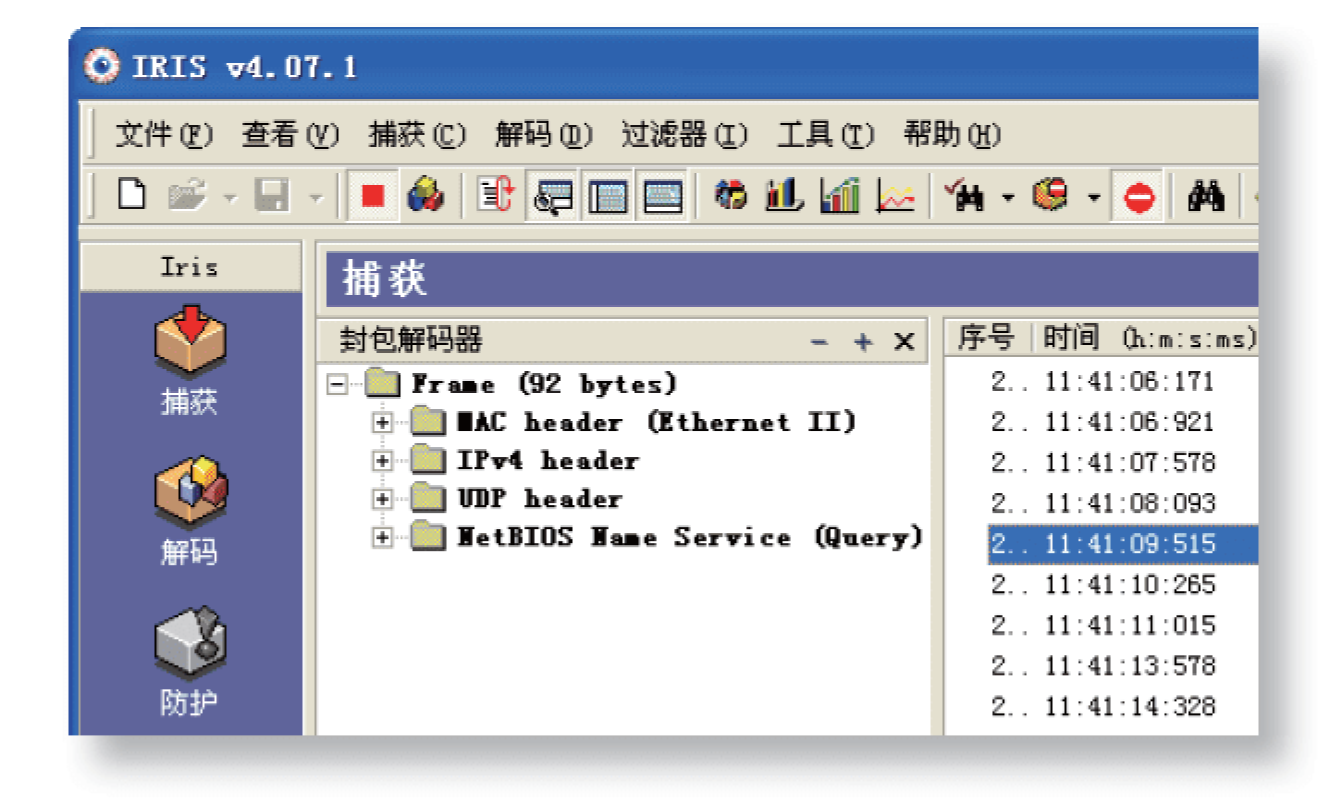
获得管理员的账户和密码即可登录系统进行数据或信息的获取和修改，使网络信息的安全受到威胁。

2. 信息共享性的利用

一些不法分子在网络中种植木马程序，如果木马程序感染了用户电脑，木马施种者就可以通过木马修改并获取用户的数据信息。

网络信息的安全将因此而没有保证，可通过在电脑中安装木马防御工具来预防木马的活动。





3. 利用软件攻击网络

在电脑中可利用软件收集网络中的信息，并且捕捉网络中电脑的物理地址或IP地址，然后通过所收集的信息攻击电脑，从而使网络信息的安全遭遇破坏。

教你一招

网络信息安全防御

要使网络信息更安全，用户在使用电脑上网时应小心谨慎，不浏览一些存在安全隐患的信息，同时在电脑中应安装相关的病毒木马防护软件。



帐号需激活后才能使用

很抱歉，您的帐号暂时不能登录。QQ安全中心启用了限制登录的保护措施，请立即点击“激活”按钮解除限制。

为什么要限制登录：

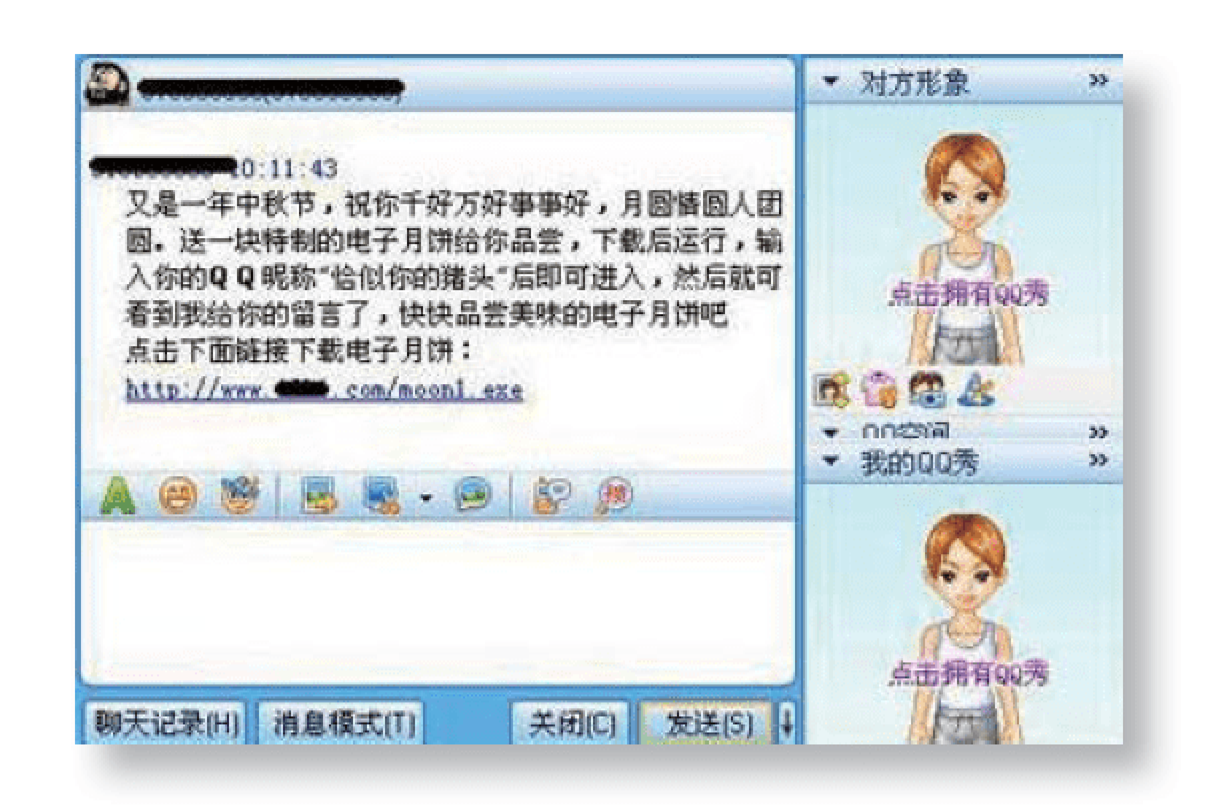
当QQ安全中心发现帐号使用异常时，将暂时限制使用，激活后才能正常登录。此措施能防止盗号者使用您的帐号从事非法行为。了解更多

4. 网络口令的泄露

泄漏网络信息操作的口令将可能使网络中的重要信息以及电脑中的机密文件被他人利用。口令的泄露主要是由于用户安全意识不强，设置的口令过于简单或者与他人共享一个ID，或者将自己的账户和口令告诉了他人。

5. 利用网络传播非法信息

一些不法分子在利用软件或其他的黑客手段获取用户的论坛或其他的聊天软件账号后，将使用其传播非法信息，这不仅给用户带来了诸多烦恼，还形成了网络信息安全的重大安全隐患，使用户对网络信息产生了极大的不安全感。对于该情况，用户需正确地判断，理智地对待。



跟我练习

认识电脑自身的安全因素

电脑自身的安全隐患同样很多，前面讲解的只是一部分典型的安全隐患，下面通过所学知识，总结电脑自身的安全因素。

任务1：收集电脑硬件的安全隐患，并了解其维护方法及标准。

任务2：总结并查询操作系统的安全隐患，针对相应的安全隐患总结出其防范措施。

任务3：结合个人信息和网络信息的安全隐患，区别其相同点和不同点，并通过上网查询了解一些防范措施。

1.3 更进一步——电脑安全技术

通过阿伟前面的讲解，娜娜已经懂得了电脑所面临的一些来自外界或自身的安全隐患。她没想到尽管电脑不大，但它所存在的威胁却这么多。阿伟感觉到娜娜好像对电脑的这些问题很在意，于是想给她讲几个电脑安全中常用的技术和方法，娜娜欣然接受了。

第1招 病毒防范技术



病毒在网络中传播扩散得很快。要杜绝网络病毒，除了要用单机防病毒产品外，还必须有适合于局域网的全方位防病毒产品。

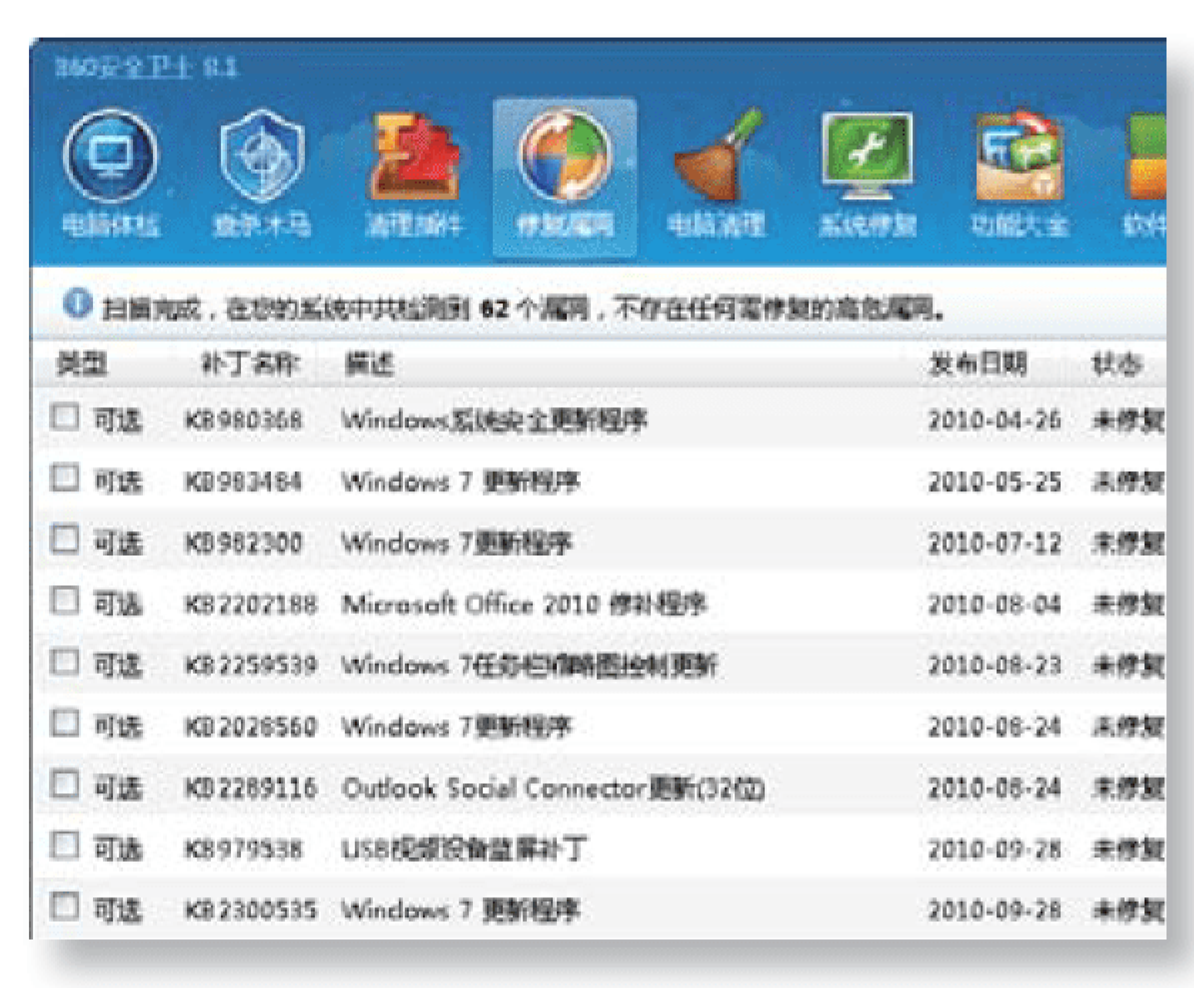
360杀毒软件是目前应用最广的免费杀毒软件之一，用户可使用其进行病毒查杀，其操作方法如下。

① 安装360杀毒软件。

② 启动其进入主界面，单击按钮快速扫描磁盘。

③ 完成扫描后，单击 X 按钮关闭窗口即可。

第2招 修复系统漏洞



电脑如果存在较多的高危系统漏洞，将很容易被黑客利用或被病毒攻击。要想减少电脑受外在因素的侵犯的可能性，应尽可能地修复系统的高危漏洞以防范不安全因素的利用。

提示：可选择目前使用最广泛的360安全卫士进行漏洞的修复，它可以智能地选择要修复的高危漏洞进行修复，同时过滤不必修复的漏洞。



第3招 充分利用防火墙

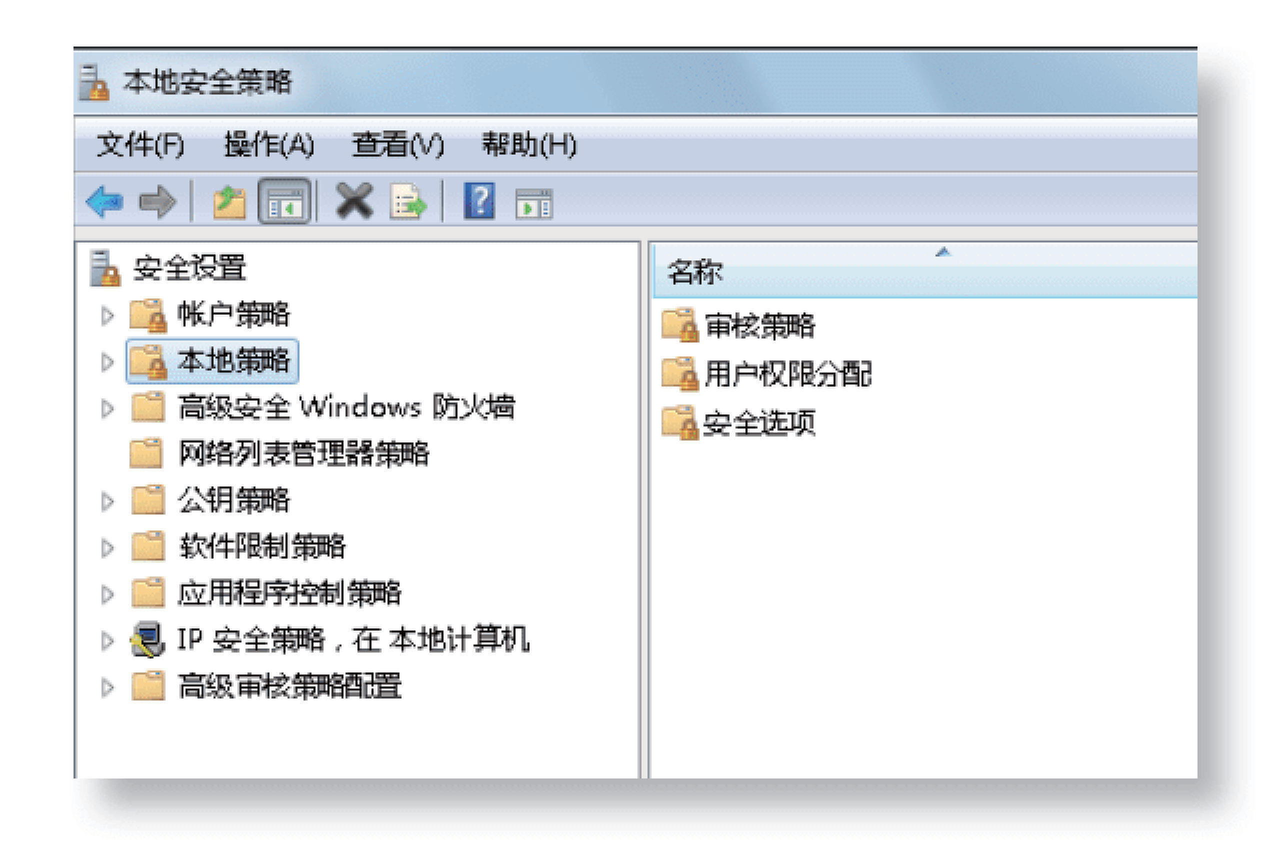
利用防火墙对网络进行访问控制设置之后，系统在运行新程序时会通知用户，从而最大限度地阻止网络中的黑客访问电脑，防止其随意更改、移动甚至删除网络上的重要信息。



提示：开启系统防火墙后，当黑客进行攻击操作时会进行拦截，并弹出通知窗口，提示用户做出相应的操作。

第4招 访问控制技术

访问控制的主要任务是保证网络资源不被非法使用和访问，是对信息系统资源进行保护的重要措施，同时也是电脑系统重要的安全机制。其主要通过设置用户的安全策略得以实现。

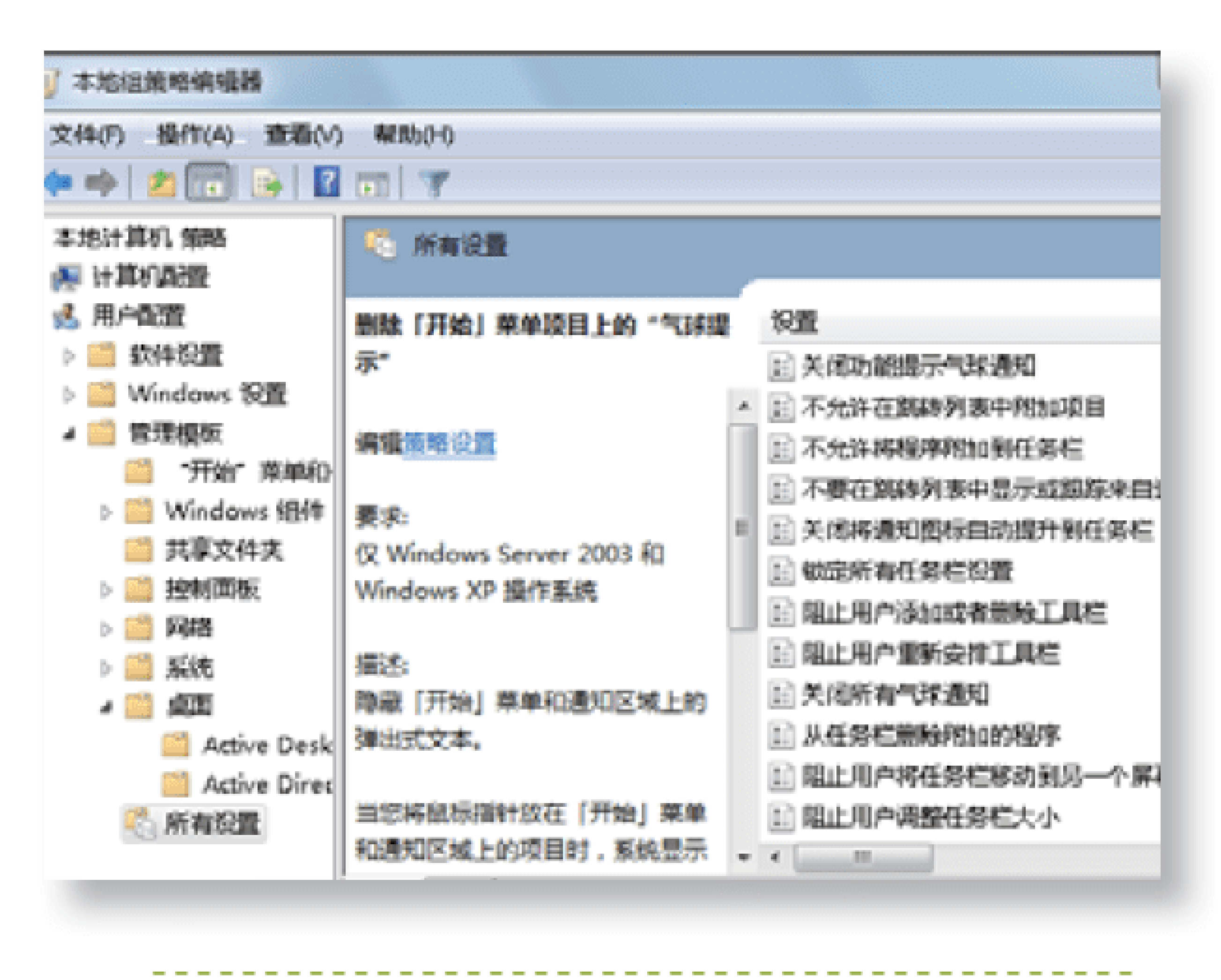


提示：设置访问控制决定了能够访问系统的用户，并且将设定访问和控制系统资源的权限。设置系统的访问控制也能阻止未经允许的用户获取数据并控制电脑的资源权限。访问控制的方法可以通过用户识别代码、口令、登录控制、资源授权、授权核查、日志和审计等来实现。

第5招 为电脑设置权限

为电脑设置权限，可以保证合法用户按照权限使用电脑系统。

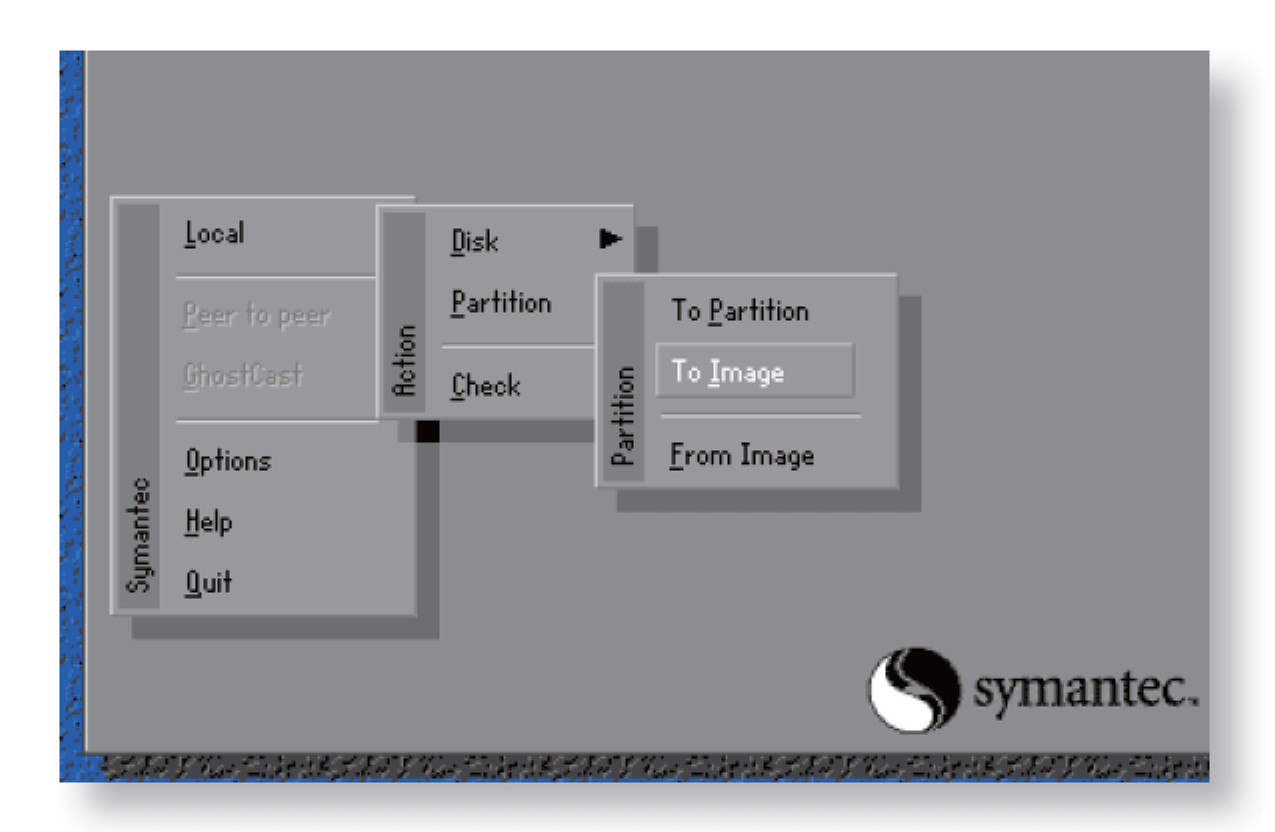
在本地组策略编辑器中可对电脑的使用权限进行设置。



第6招 备份与恢复数据

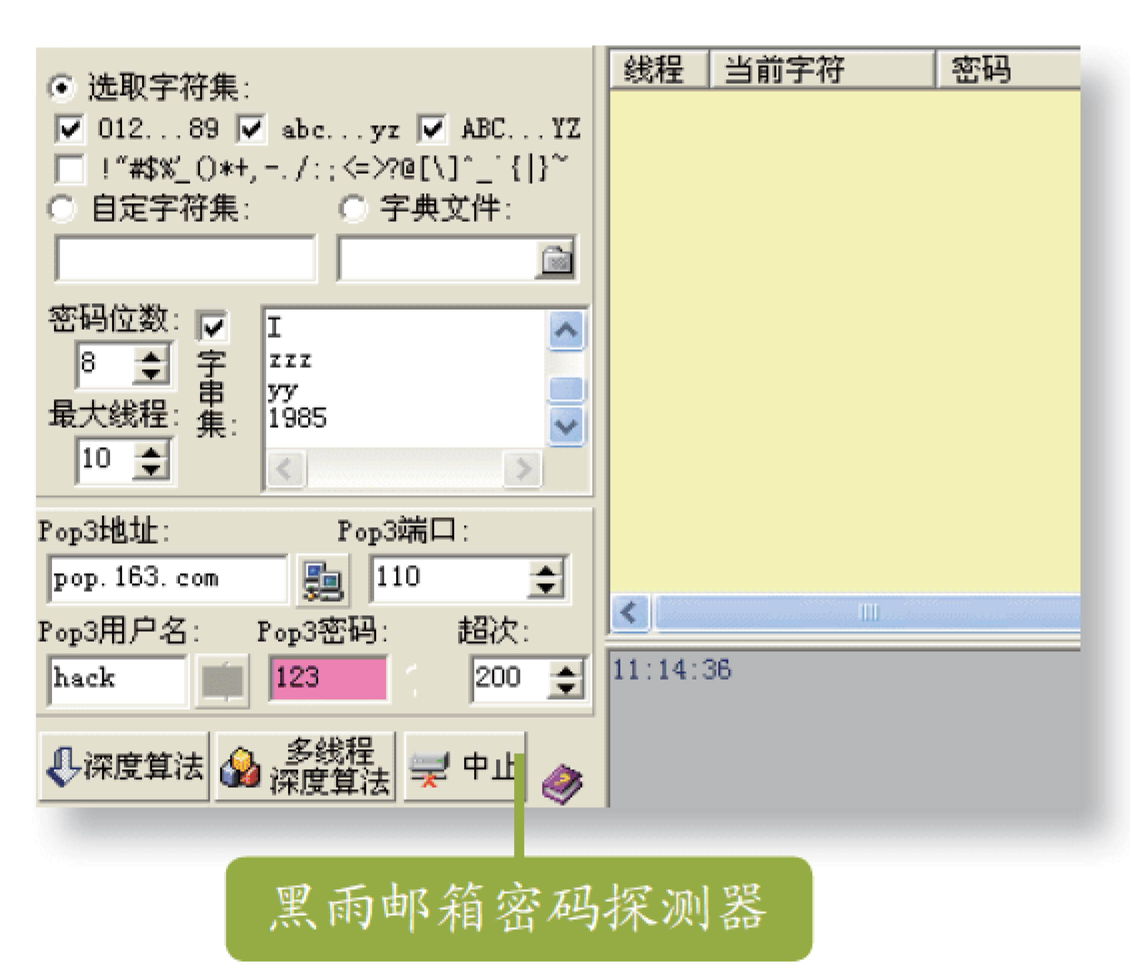
并不是所有的数据都需要备份，通常备份的是重要数据，如硬盘分区表与引导记录、操作系统等。当电脑系统被破坏时，使用备份文件即可进行恢复，从而有效保证信息的完整性。

使用Ghost软件可方便地对电脑中的重要数据进行备份。



1.5 活 学 活 用

（1）收集相关黑客软件（黑雨邮箱密码探测器）和木马病毒（冰河木马）进行使用，体验使用软件或程序对电脑进行控制和检测。



黑雨邮箱密码探测器



冰河木马

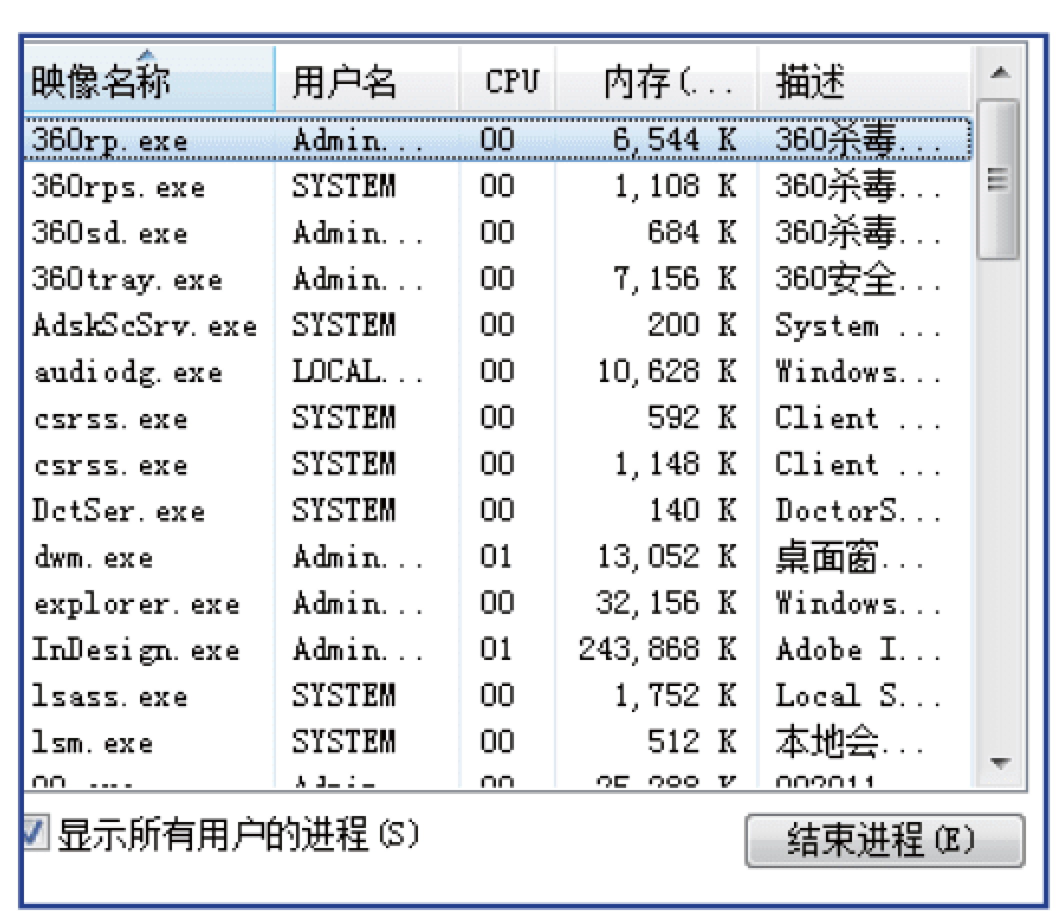


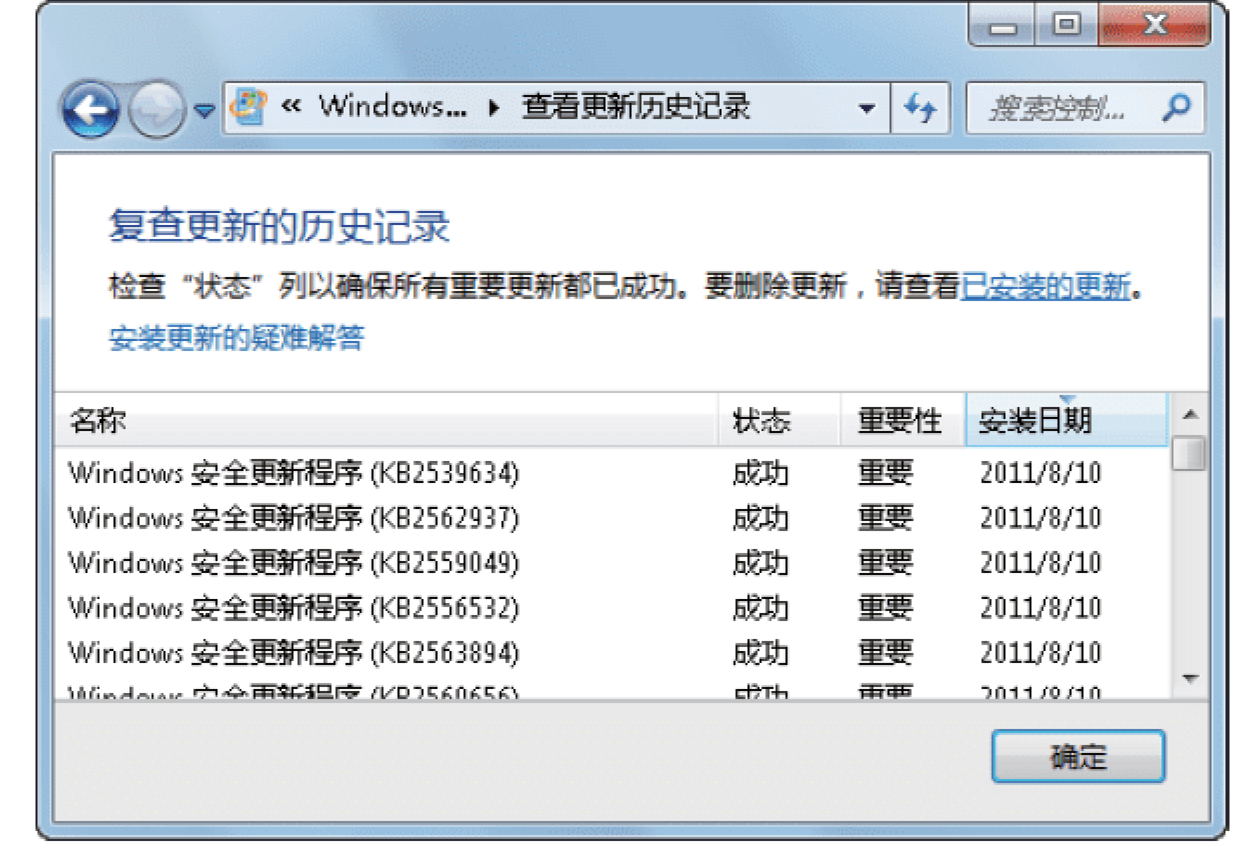
（2）使用专用工具（吹吸风机）为长期使用的电脑进行清尘，保证电脑的正常运行。在清理过程中注意不能损坏电脑的硬件。

提示：在吹风过程中，注意将其方向对准机箱后挡板有孔的地方，以确保灰尘顺利被除尽。



（3）通过所学知识，查看自己的电脑中是否存在高危漏洞，并在任务管理器中查看是否存在恶意进程。

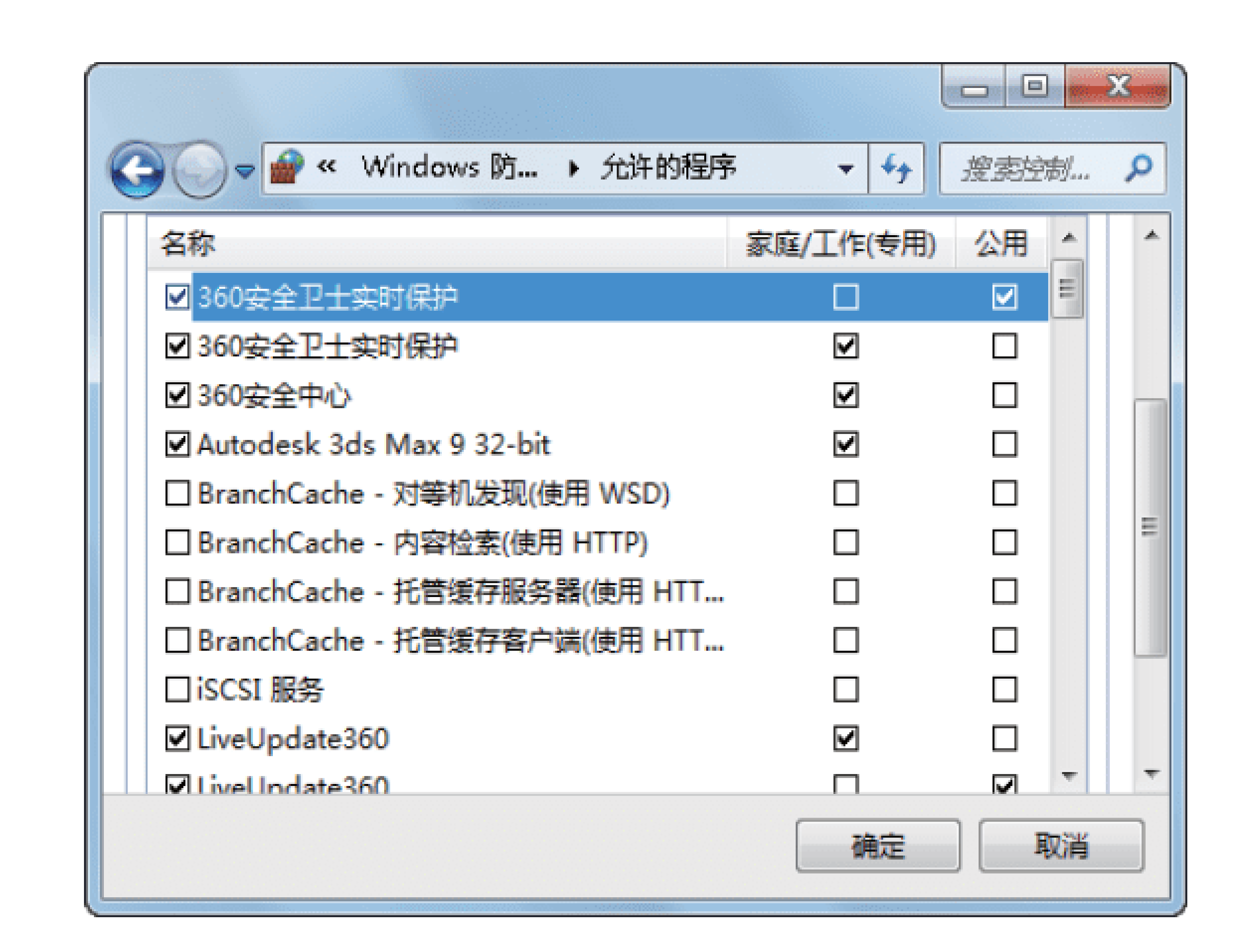




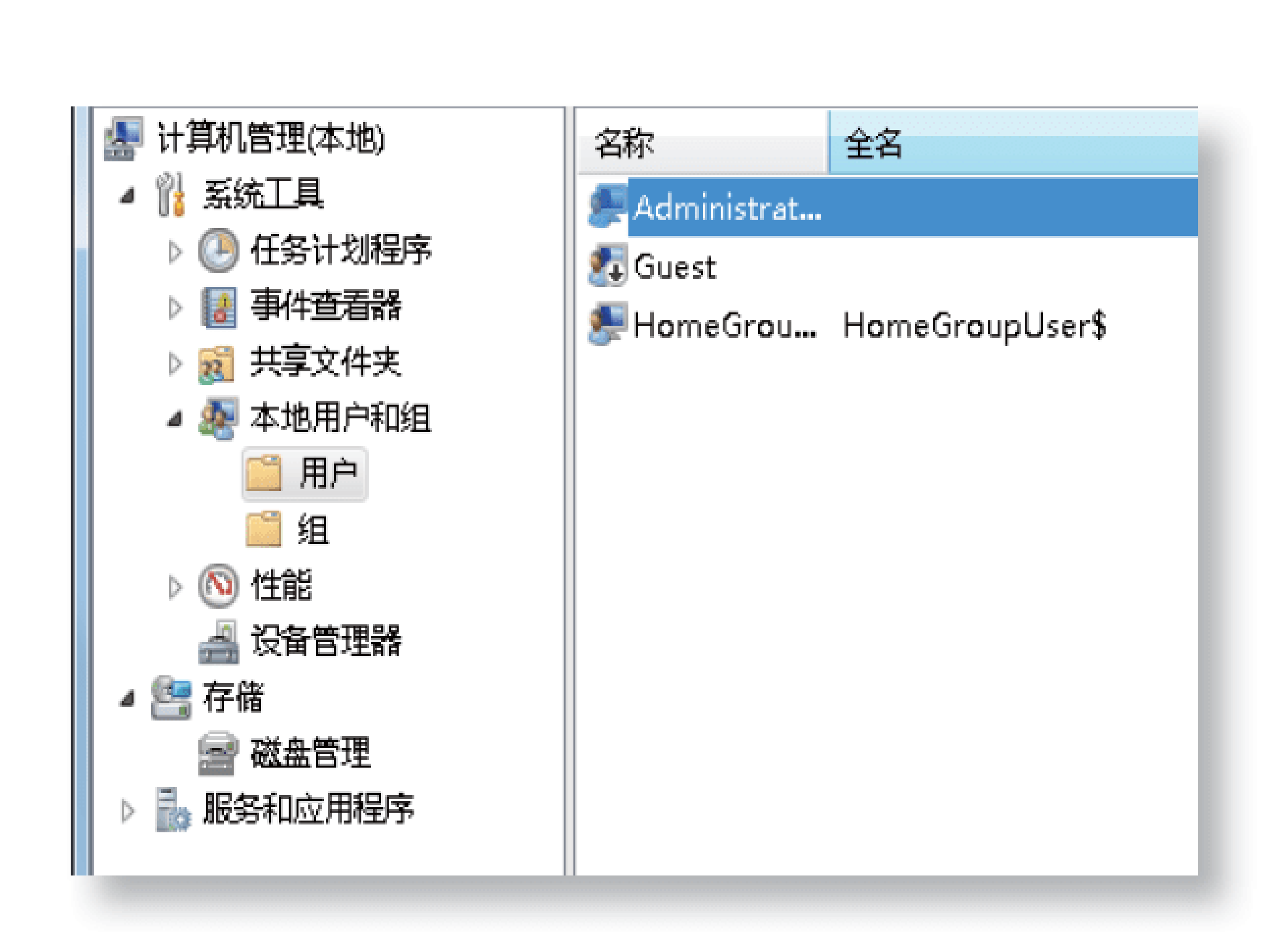
提示：除了可在操作系统中查看漏洞更新情况外，使用360安全卫士也可以查看。

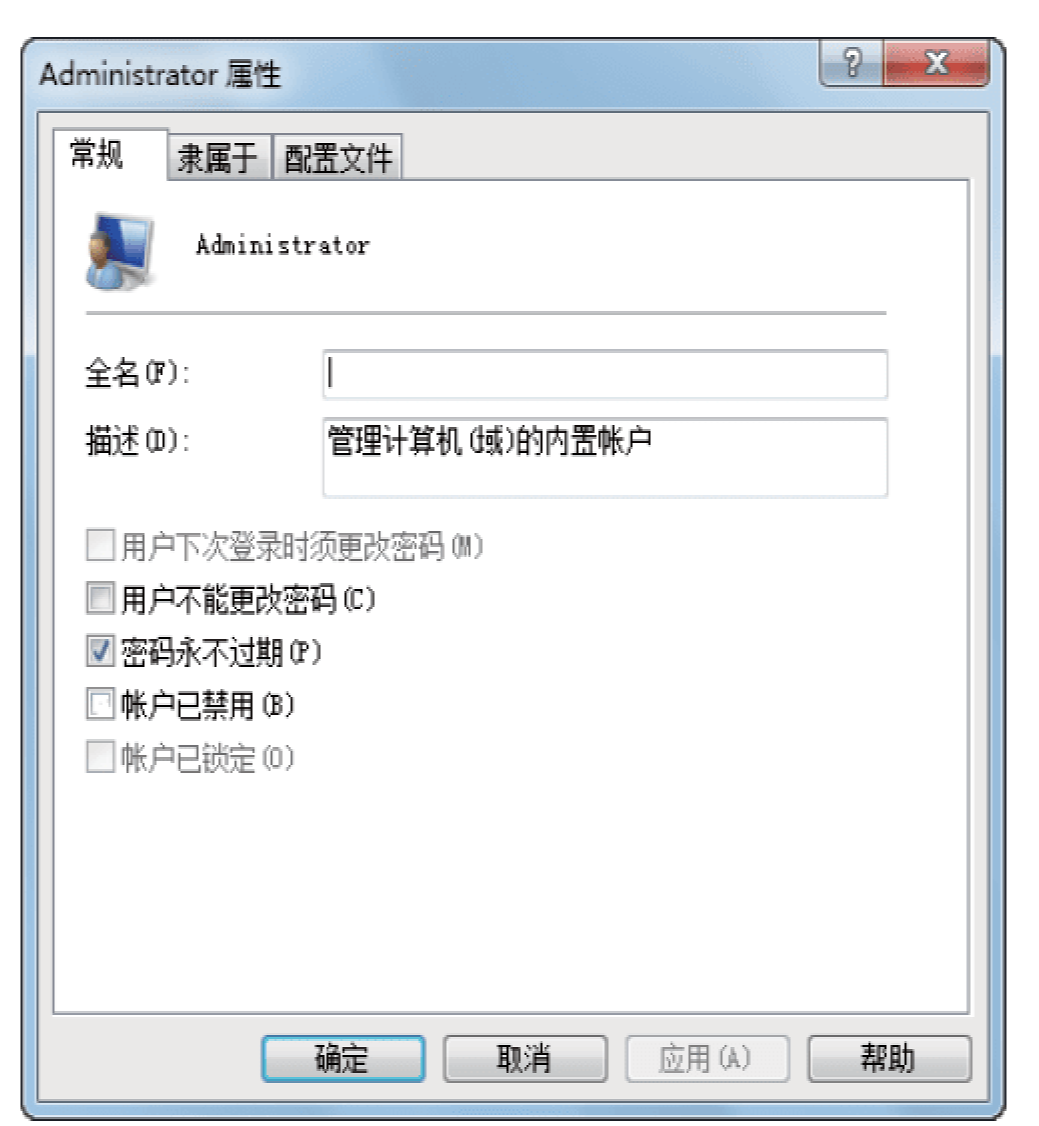
（4）在使用电脑过程中，经常会遇到安装某个应用程序时系统弹出拦截对话框。利用所学知识查看系统防火墙的防护状况。





（5）在电脑中查看管理员的安全配置是否正确，以保障网络信息的安全性。





（6）结合本章所学知识，总结黑客、病毒和木马等外界因素影响电脑安全的方式，并列举电脑自身的安全隐患。



☑ 想知道黑客都是干什么的吗？

☑ 想知道黑客攻击电脑主要是为了做什么吗？

☑ 想知道黑客是怎样攻击电脑的吗？

☑ 还在为黑客的入侵而担心吗？



第 02 章 窥探黑客攻防的秘密

阿伟给娜娜讲解了电脑所面临的威胁后，娜娜终于知道了电脑为什么会出现各种各样的“毛病”，但她却并不清楚应该怎样去解决，于是她又找到了阿伟，说：“阿伟，你能给我讲讲应该怎样去避免电脑安全问题的出现吗？”阿伟告诉她，处理电脑的安全问题应该分类进行判断，然后通过具体操作进行解决。说到这里，阿伟想到黑客对电脑的攻击，他想娜娜对这个一定很感兴趣，于是就打算先为娜娜讲解黑客的知识。

2.1　认识神秘的黑客

娜娜一直都对电影里的黑客很好奇，所以还没等阿伟休息一下就问个不停，阿伟不厌其烦地为她讲解着这些知识。为了揭开黑客的神秘面纱，阿伟打算给娜娜详细介绍一下黑客的相关知识。

2.1.1　什么是黑客

黑客，一个多么神秘的名称，人们将热心于电脑技术、水平高超的电脑专家称之为黑客，但如今的一些黑客对别人的电脑大肆进行恶意破坏。因此，它也成了对那些专门利用电脑网络搞破坏的一类人的称呼。



黑客对于人们不再陌生，我们知道，黑客在电脑方面具有高超的技能，在网络上无所不能，通常可按黑客的不同主攻对象将其进行分类，下面将对其进行介绍。

- **黑帽黑客：**“黑帽黑客”也称为“骇客”，是指恶意试图破解或破坏某个程序、系统及网络安全的人。这样的黑客常常对那些创造或编写软件的黑客造成严重困扰。
- **白帽黑客：**“白帽黑客”也称为“匿名客”（sneaker）或“红客”，是指寻找某系统或网络的漏洞进行破解，以提醒该系统所有者的系统安全漏洞的人。这样的人大多是电脑安全公司的雇员，他们在完全合法的情况下攻击某系统。

新手解惑

Q：黑客有什么共同点吗？

A：不管是黑帽黑客还是白帽黑客，他们都是对于某领域内的编程语言很精通、能轻易创造出有价值的软件的人。

2.1.2　黑客攻击的目的和行为准则

黑客具有随意入侵别人的电脑查看信息，然后悄然退出的能力。很多人对他们有极强的崇拜心理，并产生了极高的学习黑客技术的欲望，他们进行攻击都怀有一定的目的。但真正的黑客其实有着一套行为准则，下面将对黑客攻击电脑的目的和行为准则分别进行介绍。



1. 攻击目的

黑客可以来去自如地进入别人的电脑、浏览别人电脑内的文件、破解机密信息、传播病毒木马、造成别人电脑系统崩溃和硬盘分区表损坏等，其都带有一定的目的性。



黑客的攻击目的主要有以下几种。

- **进程的执行：**如果黑客在连接到目标主机后，网络中有一个站点能够访问另一个严格受控的站点或网络，黑客为了攻击这个站点或网络，可能会首先攻击这个中间的站点。
- **获取文件和传输中的数据：**黑客登录目标主机或使用网络监听进行攻击时，通常将复制当前用户目录下的文件系统中的用户名或密码。
- **获取超级用户的权限：**在一个局域网中，掌握了一台主机的超级用户权限，才能掌握整个子网。
- **对系统的非法访问：**黑客通常对系统进行攻击，以一种非法的行为来得到访问的权限。
- **进行不许可的操作：**许多黑客都会去尝试尽量获取超出允许的一些权限，于是便寻找管理员在设置中的漏洞，或者去找一些工具来突破系统的安全防线。
- **拒绝服务：**一种有目的的破坏行为，其攻击方式包括将连接局域网的电缆接地；在网络中制造大量的封包，占据网络的带宽并延缓网络的传输等。
- **涂改信息：**对重要文件修改、更换和删除的恶劣攻击行为。

教你一招

黑客使用系统工具可能暴露自身信息

黑客攻击时，如果使用一些系统工具，往往会被记录下来发送到指定的站点，这样可能会暴露黑客的身份和地址。

2. 黑客行为准则

现在黑客的概念越来越模糊，一些会偷QQ密码的都能自称是黑客，挂几个肉鸡攻击他人站点的也称作是黑客，其实他们都不是，黑客作为一个特殊的群体，也有一些默认的守则，真正的黑客应该具备一定的精神与素质。



黑客遵守的准则有以下几点。

- 不侵入破坏政府机关的主机或攻击电信和各种正常网站的主机。
- 不恶意破坏任何系统和文件数据。
- 不修改任何系统文件，如果目的是为了要进入系统而修改它，那么要在达到目的后将其还原。
- 不公开已破解的账号，不轻易将要攻击的站点告诉其他人。不在网络上谈论关于黑客攻击的任何事情，编写文章时不要使用真名。
- 不修改系统文件，如果为了隐藏自己的侵入而作的修改则不在此限，但仍需维持原来系统的安全性，不因得到系统的控制权而破坏原有的安全性。
- 不断地解决各种电脑问题，不断地发现新的电脑问题，帮忙测试和处理软件缺陷。
- 公布有用的信息帮助维持网络和电脑的一些简单工作。有好的心理素质和正确的世界观。有明确的人生目标，并为之努力奋斗。

2.2 黑客攻击原理

阿伟告诉娜娜，因特网并不是一个单独的、封闭的网络，它是建立在全球众多网络上的一个网络集合。在因特网上存在许多不同类型的电脑及运行各种系统的服务器。黑客利用TCP/IP协议在网络上传送包含有非法目的合法数据，对网络上的电脑进行攻击。

新手解惑

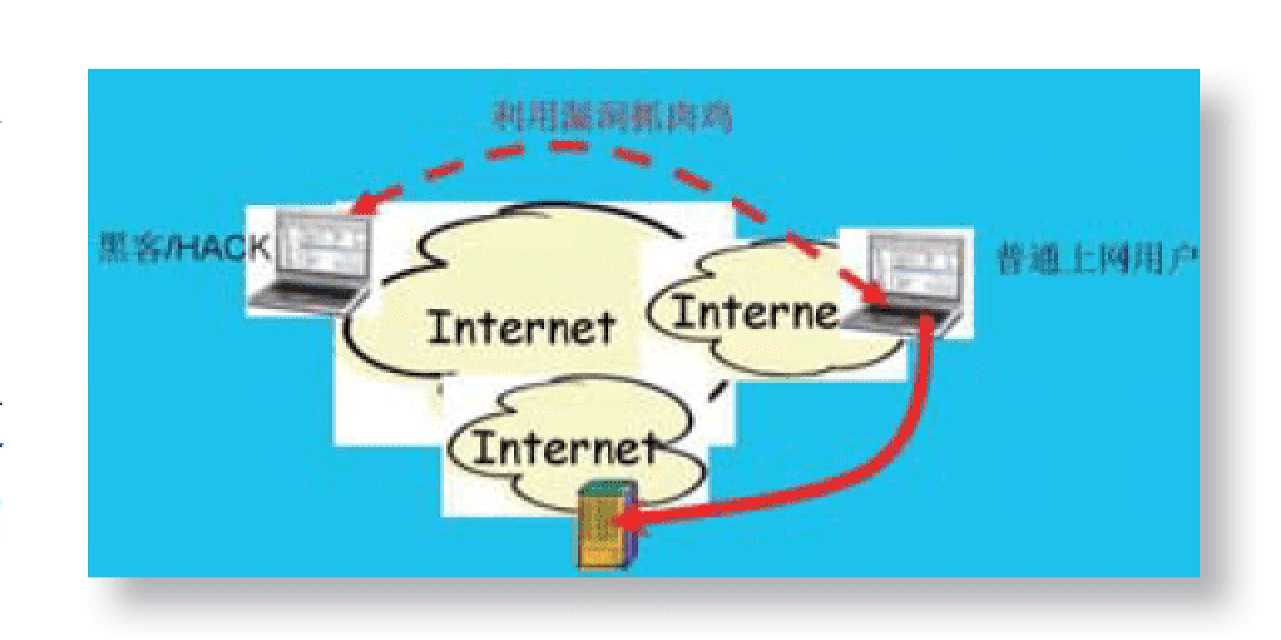
Q：什么是TCP/IP协议？它有什么作用？

A：TCP/IP协议是将电脑组成网络的一系列协议的总和，TCP协议，称为传输控制协议，IP协议，称为网间互联协议。TCP/IP协议能够确保不同类型的电脑及网络在一起工作。



黑客通过系统中存在的漏洞侵入目标电脑，控制此台电脑并将其作为自身攻击其他电脑的掩饰，继续寻找网络中其他电脑或服务器。

当被攻击电脑发现时，进行寻找攻击的来源，将显示被黑客控制的电脑的信息，而真正的黑客已经逃之夭夭。



2.3 常见黑客命令的使用

初步认识了黑客的基础知识后，阿伟打算给娜娜讲解一些关于黑客命令的用法，只有知己知彼，才能百战不殆。因此，掌握黑客的命令对于防范黑客攻击有着很大的帮助。娜娜了解了阿伟的想法后，已经迫不及待地要求阿伟为她讲解了。

2.3.1 ping命令的使用

ping命令是黑客使用最频繁的命令之一，使用ping命令可测试目标主机的主机名、IP地址信息以及验证本地主机与远程主机的连接。



下面将对使用ping命令查看IP信息的方法进行介绍，其具体操作如下。



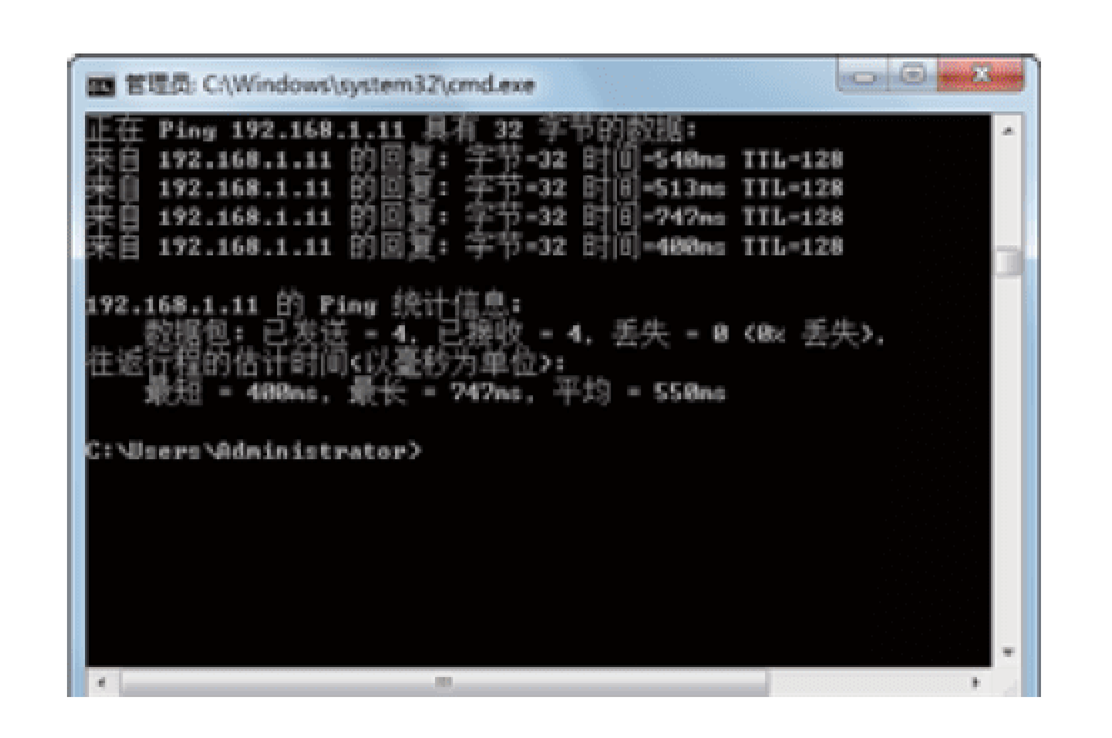
第1步：打开命令提示符窗口

选择“开始”/“运行”命令，在打开的“运行”对话框的“打开”下拉列表框中输入“cmd”，然后单击确定按钮，即可打开命令提示符窗口。

新手解惑

Q：为什么我的“开始”菜单中没有“运行”命令？

A：默认没有显示该命令，当使用频率较高时才显示出来。在“开始”菜单空白处单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开的对话框中选择“「开始」菜单”选项卡，单击自定义(C)...按钮，在打开的对话框中选中“运行命令”复选框，保存设置即可。



第2步： 查看IP信息

在命令提示符中输入“ping WIN-JGPQBQH7SVF”命令，其中“WIN-JGPQBQH7SVF”为具体的计算机名称，然后按Enter键，即可显示该电脑的IP地址。

教你一招

ping命令的格式

ping命令的格式为：ping+参数，其主要参数有 -t、-a、-n count、-l length、-f、-i ttl、-v tos、-r count、-s count、-j computer-list、-k computer-list、-w timeout destination和-list。

常见ping命令的参数及其含义

参　数	含　义
-t	一直ping指定的电脑，直到按Ctrl+C键中断
-a	将地址解析为电脑NetBios名
-i ttl	将“生存时间”字段设置为ttl指定的值
-n count	发送count指定的ECHO数据包数，能够测试发送数据包的返回平均时间及时间的快慢程度，默认值为4
-f	在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段
-r count	在“记录路由”字段中记录传出和返回数据包的路由，指定的count值最大为9，最小为1
-s count	指定count 指定的跃点数的时间戳。此参数不记录数据包返回所经过的路由，最多只记录4个
-w timeout destination	指定超时间隔，单位为“毫秒”

2.3.2　ipconfig命令的使用

ipconfig命令主要用于显示电脑中网络适配器的IP地址、子网掩码以及默认网关，是Windows操作系统中调试电脑网络的常用命令。





下面将使用ipconfig命令查看电脑的IP地址、子网掩码以及默认网关，其具体操作如下。

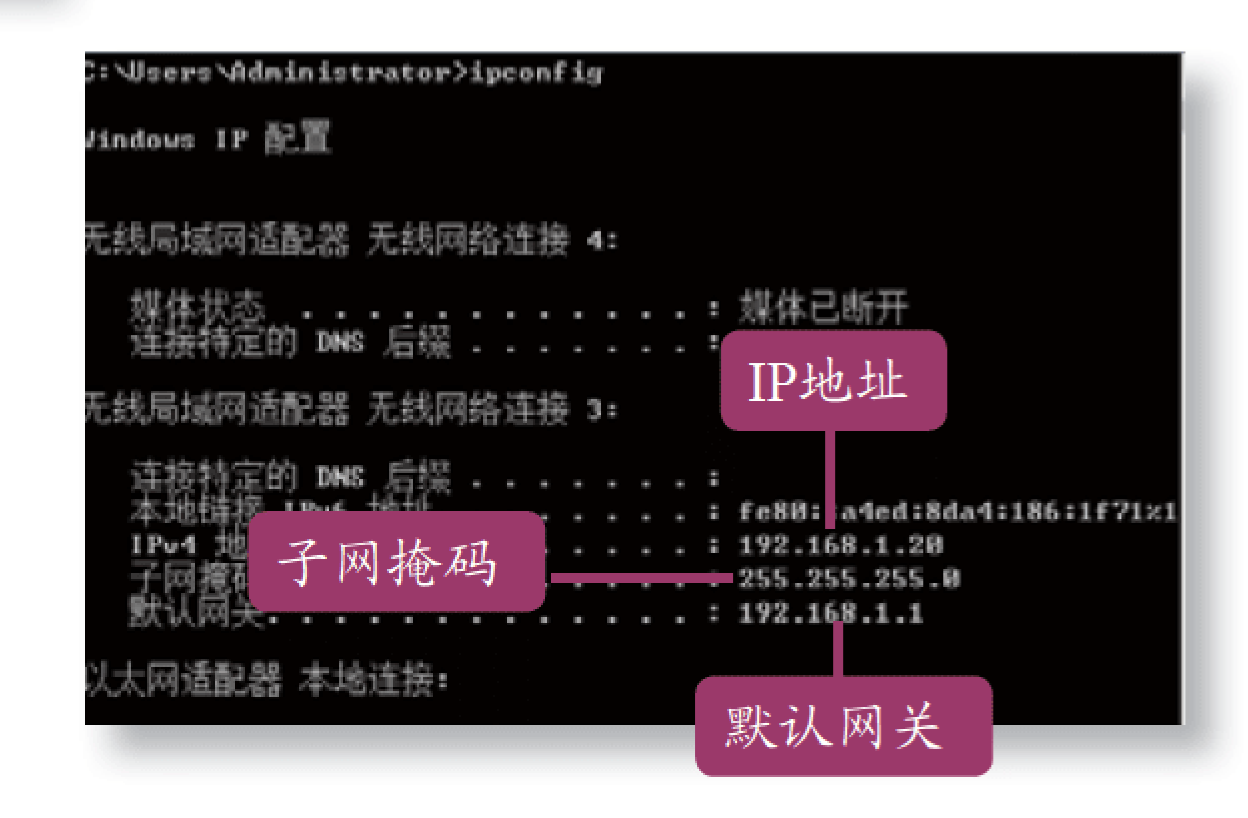


第1步：打开命令提示符

选择“开始”/“运行”命令，在打开的“运行”对话框的“打开”下拉列表框中输入“cmd”，单击 确定 按钮，打开命令提示符。

第2步：查看电脑信息

在命令提示符中输入“ipconfig”命令，按Enter键，当前主机的IP信息、默认网关以及子网掩码将会显示在其中。



教你一招

使用ipconfig的技巧

ipconfig有多种用法，在其后接不同的参数其作用不同。

无参数：使用ipconfig时不带任何参数，可查询每个已经配置的接口显示IP地址、子网掩码和默认网关值。

/all：显示完整的TCP/IP配置信息。与不带参数的用法相比，其信息更全，如IP是否动态分配、显示网卡的物理地址等。

/batch：将ipconfig所显示信息以文本方式写入指定文件。此参数可用来备份本机的网络配置。

/release：释放全部适配器由DHCP分配的动态IP 地址。此参数适用于IP地址非静态分配的网卡，通常和renew参数结合使用。

/renew：为全部适配器重新分配IP地址。此参数同样仅适用于IP地址非静态分配的网卡。

2.3.3 net命令的使用

net命令通常可用于管理电脑的网络环境和各种服务程序的运行与配置。使用其附加命令，可管理网络环境、服务、用户和登录等重要的功能。



下面将介绍一些常用net附加命令的基本功能。

- net view：主要用于显示网络中域列表、电脑列表或指定电脑的共享资源列表的命令。
- net user：用于添加或更改用户账号或显示用户账号信息。
- net share：用于创建、删除或显示共享资源。
- net use：用于连接或断开电脑与网络中共享资源的连接以及显示电脑连接的相关信息。
- net start：用于启动服务或显示已启动服务的列表命令。
- net stop：用于停止Windows操作系统中网络服务的命令。
- net localgroup：用于查看所有和用户组的相关信息，同时使用该命令可以相同或相似方式将使用电脑或网络的用户分组，在对本地组指派权限时，本地组的每个成员都自动获得相同的权限。

教你一招

使用net命令的注意事项及其特殊功能

使用net命令应注意区分“域”和“工作组”这两个概念的用法：域是指一种服务器控制网络上电脑能否加入的电脑组合；工作组则是操作系统中将不同电脑按功能和用途划分的不同类型组。

net命令具有强制参数的功能，所有net命令接受选项/yes和/no（可缩写为/y和/n），也就是预先给系统的提问给出答案。

2.3.4 netstat命令的使用

netstat命令基于TCP/IP协议，即只有安装了TCP/IP协议才能使用，它是Windows操作系统自带的查看网络状况的命令。



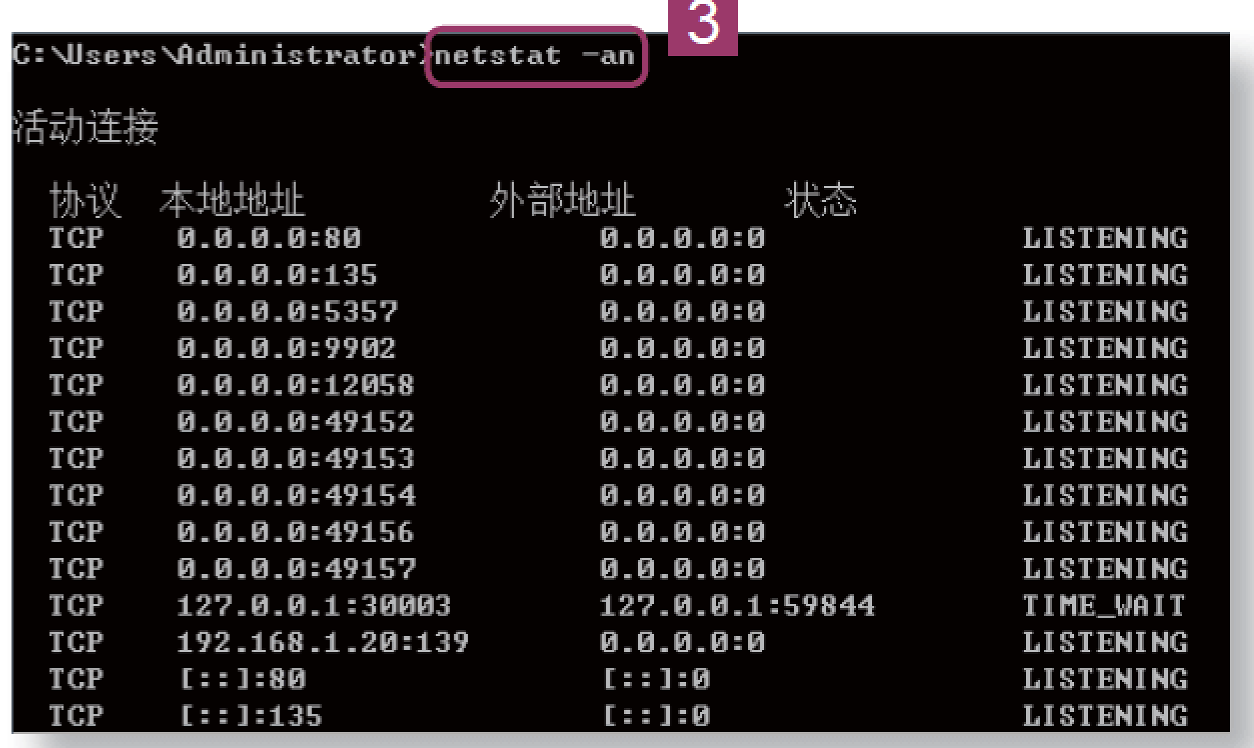


下面将使用netstat命令查看本地电脑开放的端口信息，其具体操作如下。



第1步：打开命令提示符

选择“开始”/“运行”命令，在打开的“运行”对话框的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。



第2步：查看端口信息

在打开的命令提示符窗口中输入“netstat -an”，按Enter键即可查看本地电脑所开放的端口信息。

常见netstat命令的参数及其作用

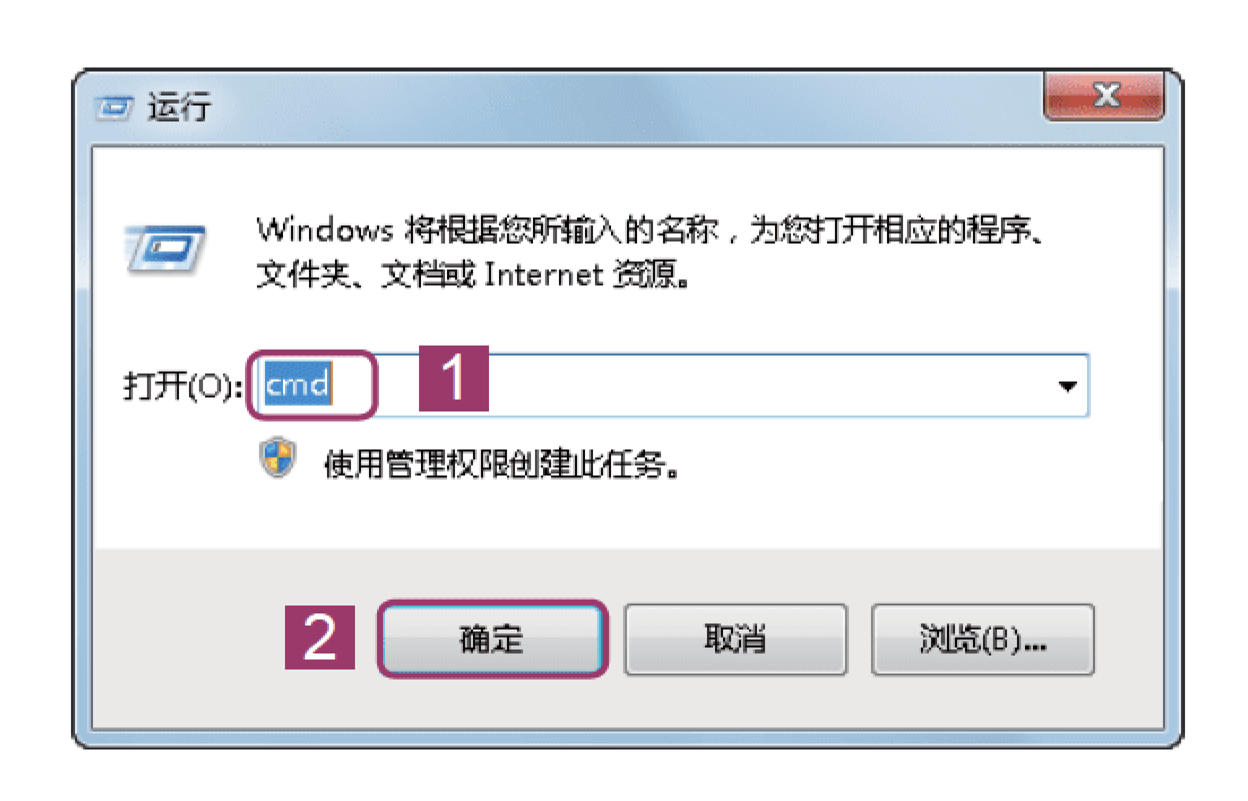
参数	作用
-a	显示所有连接和监听的端口
-e	显示以太网端口，它可与-s合用
-n	以数字格式显示地址和端口号
-o	显示活动的TCP连接并包括每个连接的进程ID，它可与-a、-n合用
-s	显示每个协议的统计
-p protocol	显示由protocol指定的协议的连接，如与-s合用则显示每个协议的统计
-r	显示路由表的内容
-Interval	重新显示所选的统计，可指定在每次显示之间暂停的时间，按Ctrl+C键即可停止重新显示统计

2.3.5 tracert命令的使用

使用tracert命令可搜集目标网站的结构信息，它是Windows操作系统自带的路由跟踪命令，通过该命令返回的结果可获取从本机发送数据包到目标主机所经过的网络设备，得知其传送路径。



下面将使用tracert命令搜集百度结构信息，其具体操作如下。

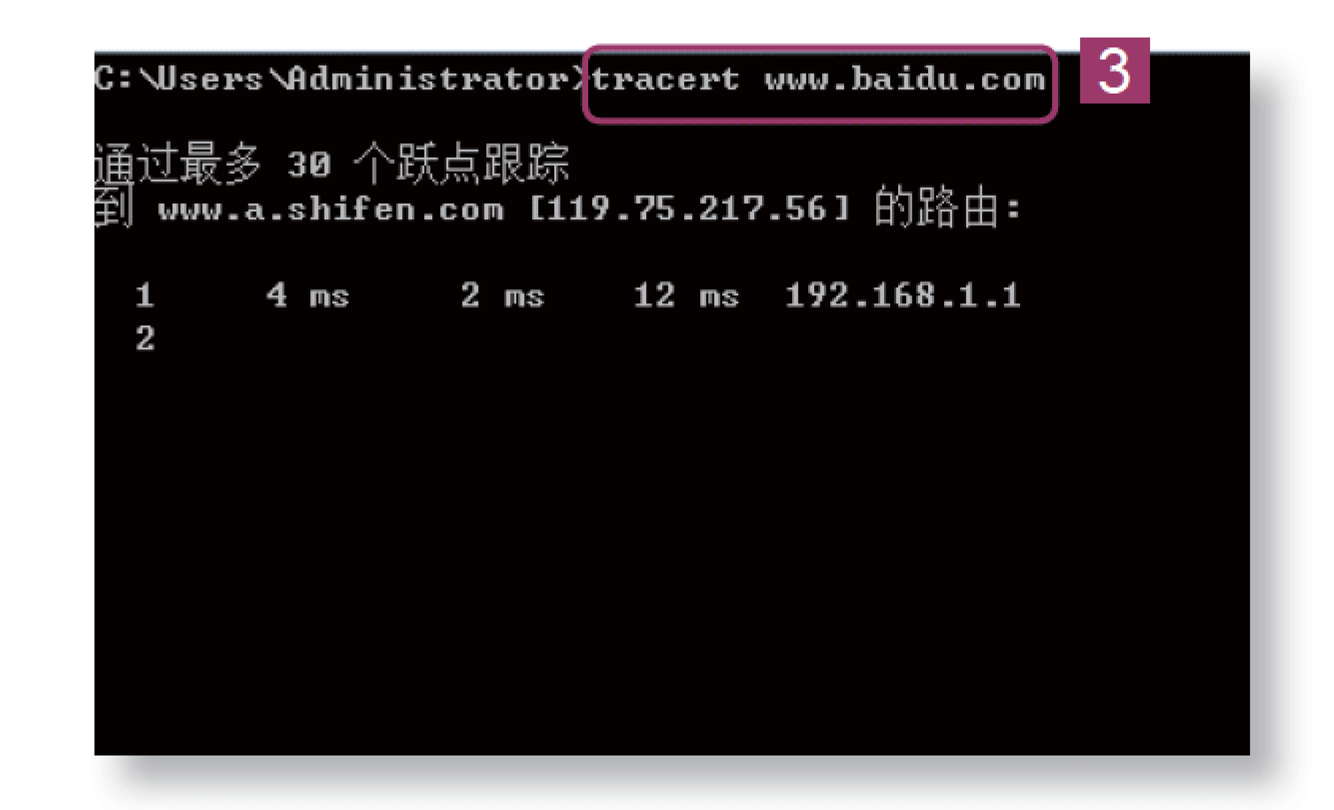


第1步：打开命令提示符

选择“开始”/“运行”命令，在打开的“运行”对话框的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

第2步：获取网站信息

在打开的命令提示符窗口中输入“tracert www.baidu.com”命令，按Enter键，在返回的结果中即可知道数据包经过的节点。



教你一招

其他常用命令的使用方法

使用telnet+空格+IP地址/主机名称命令，可以直接使用Telnet协议在远程电脑之间进行通信，就像登录到本地电脑上执行命令一样。

使用ftp命令可使文件传送协议在本地和远程主机或远程主机之间传送文件，以实现文件的上传功能。



跟我练习

使用学过的黑客命令获取电脑的相关信息

任务1：使用ping命令查看网络中的连接状况。

任务2：使用ipconfig命令释放并重新获取IP地址。

任务3：使用tracert命令收集新浪的结构信息。

```
C:\Users\Administrator>ping 192.168.1.11 -t

正在 Ping 192.168.1.11 具有 32 字节的数据:
来自 192.168.1.11 的回复: 字节=32 时间=7ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=4ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=10ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=7ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=7ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=18ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=5ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=8ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=3ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=4ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=5ms TTL=128
来自 192.168.1.11 的回复: 字节=32 时间=6ms TTL=128
```

```
C:\Users\Administrator>ipconfig /release

Windows IP 配置

不能在 无线网络连接 4 上执行任何操作，它已断开媒体
不能在 本地连接 上执行任何操作，它已断开媒体连接。

C:\Users\Administrator>
```

2.4 怎样防范黑客攻击

娜娜问阿伟："那我怎样做可以防止黑客的攻击呢？"阿伟告诉娜娜，在使用电脑的过程中，采取一些防范措施可以减少甚至杜绝黑客攻击，如关闭端口、使用防火墙、隐藏IP地址、减少用户账户和确认网上交易的正确等。接下来阿伟就认真地给娜娜讲解起来。

2.4.1 关闭端口

端口既是电脑通信的通道，同时也是黑客入侵的通道。黑客在对电脑进行扫描时，扫描的对象几乎包括了电脑所有的端口，特别是一些闲置不用的端口，黑客就专门利用这些端口进行攻击。

1. 易受黑客攻击的端口

在电脑中可关闭制定服务的端口，此时电脑将不会收到具有针对性的攻击，电脑中存在很多容易遭受黑客攻击的端口。



下面将对电脑中容易受到黑客攻击的端口，以及各端口提供的服务进行介绍。

易受黑客攻击的端口

端口号	服务	受到的攻击
25	SMTP服务	发送垃圾邮件信号
53	DNS	攻击防火墙或LAN配置
57	E-mail	查找Web服务器的弱点
67	引导程序	攻击设备
135和445	Windows RPC	感染最新的Windows病毒或蠕虫病毒
161	SNMP服务	控制路由器、防火墙或交换机
1433	SQL服务	感染SQL slammer蠕虫病毒
2847	诺顿反病毒服务	攻击电脑设置

2. 定向关闭服务端口

在控制面板中打开管理工具即可启动系统服务，通常可关闭FTP服务、DNS服务和Telnet服务等。



下面通过控制面板中的服务选项关闭相关服务，其具体操作如下。



第1步：打开控制面板

在系统桌面上选择“开始”/“控制面板”命令，即可打开“控制面板”窗口。

第2步：打开“服务”对话框

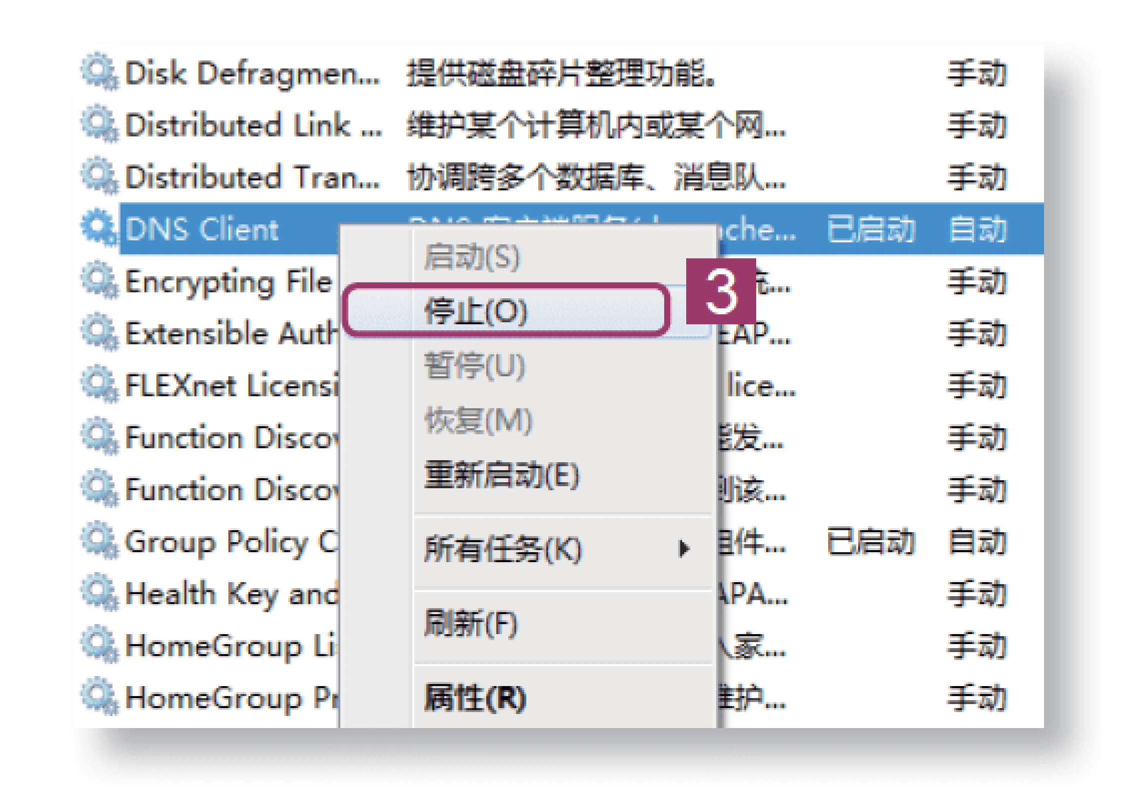
在控制面板中单击“管理工具”超链接，即可打开“管理工具”窗口，在其中双击“服务”选项，打开“服务”对话框。

iSCSI 发起程序	2009/7/14 12:41	快捷方式
Windows PowerShell Modules	2009/7/14 12:52	快捷方式
Windows 内存诊断	2009/7/14 12:41	快捷方式
本地安全策略	2011/9/17 1:35	快捷方式
打印管理	2011/9/17 1:34	快捷方式
服务 2	2009/7/14 12:41	快捷方式
高级安全 Windows 防火墙	2009/7/14 12:41	快捷方式
计算机管理	2009/7/14 12:41	快捷方式
任务计划程序	2009/7/14 12:42	快捷方式
事件查看器	2009/7/14 12:42	快捷方式
数据源(ODBC)	2009/7/14 12:41	快捷方式
系统配置	2009/7/14 12:41	快捷方式
性能监视器	2009/7/14 12:41	快捷方式



第3步：关闭相关服务

在打开的对话框中要关闭的服务选项上单击鼠标右键，在弹出的快捷菜单中选择“停止”命令，即可关闭该服务选项。



2.4.2 使用防火墙

黑客扫描端口，正常的操作是屏蔽该端口，查找黑客正在扫描的端口，通过用户手动操作是不可能完成的，需要通过软件来完成，这类软件就是常用的网络防火墙。网络防火墙的工作原理是检查所有传输到电脑中的数据包，并有完全的否决权，可以禁止接收网络中的有害事物。



这里以天网防火墙为例讲解网络防火墙屏蔽端口的方法，其具体操作如下。



第1步：浏览天网防火墙基本信息

运行天网防火墙，在其主界面上可查看软件的默认设置，这里自定义为开机后自动启动防火墙，并自动监测本机的IP地址信息等。

第2步：禁止连接低端串口

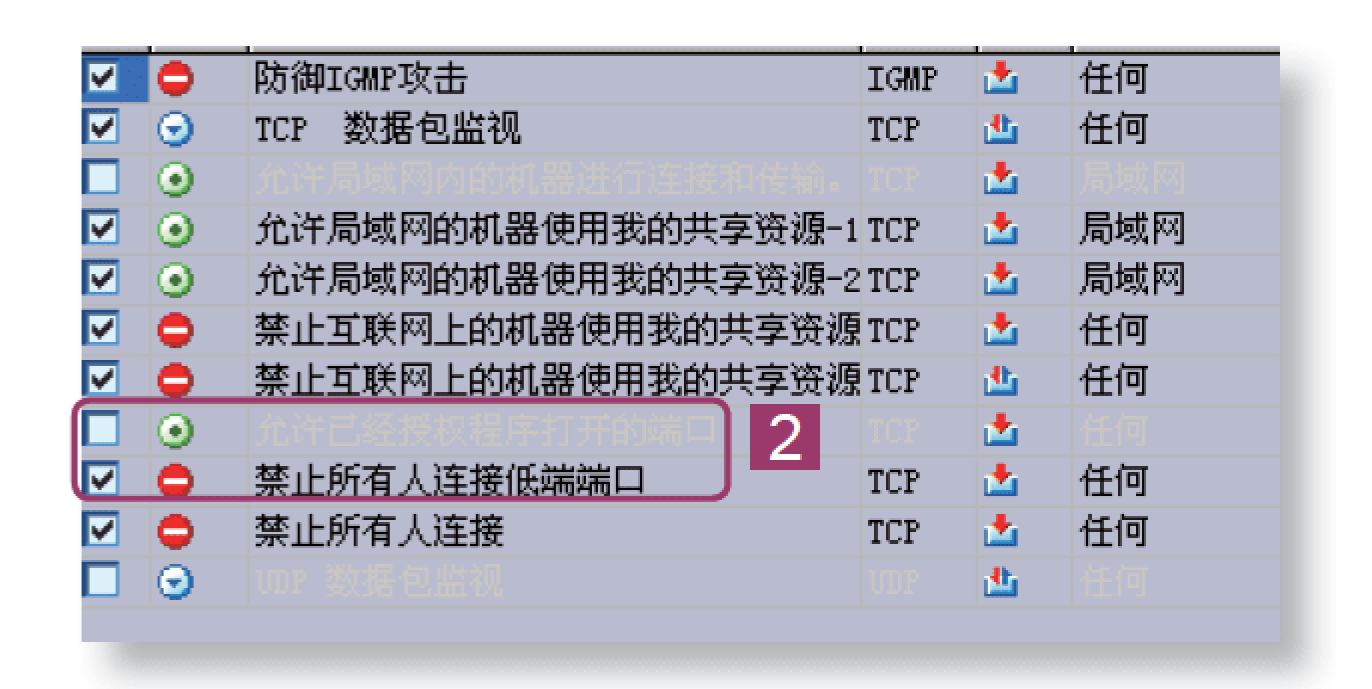
单击按钮，进入IP规则设置界面，在其中可自定义IP规则。

提示：在“自定义IP规则”窗口中，当取消选中某一复选框时，其复选框对应的选项呈灰色显示。



第3步：屏蔽端口

在“自定义IP规则”列表框中选中“禁止所有人连接低端端口”复选框，取消选中“允许已经授权程序打开的端口”复选框。



2.4.3 隐藏IP地址

黑客通过扫描网络中主机的IP地址进入电脑，以获得主机信息。将主机的IP地址隐藏起来就是最好的预防扫描的方法。

新手解惑

Q：隐藏IP地址的方法是什么？IP地址是怎样进行隐藏的？

A：用户隐藏IP地址可通过使用代理服务器来实现。使用网络浏览器直接连接Internet站点取得网络信息时，通常直接连接到目的站点服务器，然后由目的站点服务器把信息传送回来。

浏览器不是直接到Web服务器取回网页，而是向代理服务器发出请求，信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给浏览器。因此，使用代理服务器后，黑客扫描的IP地址是代理服务器的，不是电脑真正的IP地址，这样就实现了隐藏IP地址的目的，从而有效预防黑客扫描。



下面将通过浏览器在网页中设置代理服务器，从而避免黑客找到自己的IP地址，其具体操作如下。

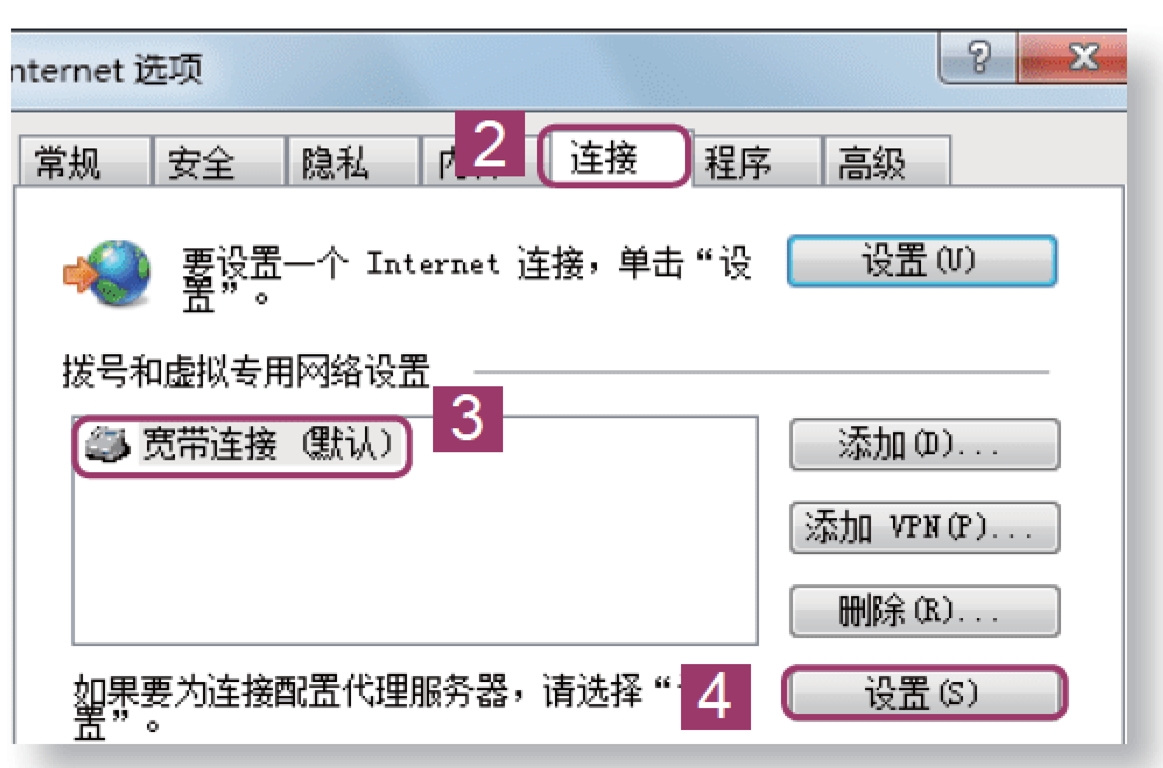




第1步：打开“Internet 选项”对话框

启动浏览器，选择“工具”/“Internet 选项”命令，打开“Internet 选项”对话框。

提示：代理服务器可以在代理服务器发布站（http://www.okeydown.com/article/info/1047.html）里找到，有最新的代理服务器列表，如找到一个代理服务器：158.43.128.51:3128@HTTP，那么这个代理服务器的IP地址就是：158.43.128.51，端口号为：3128。

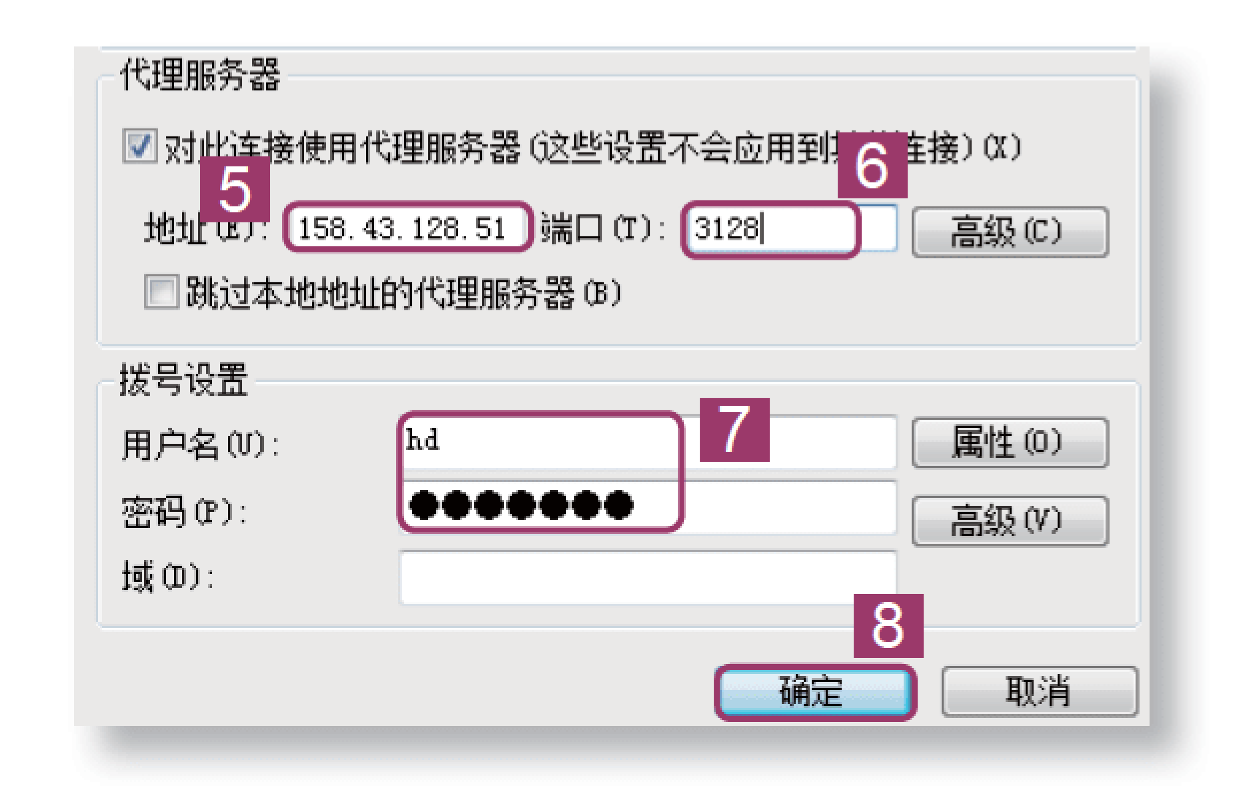


第2步：选择使用代理服务器的选项

在打开的对话框中选择“连接”选项卡，在其中的列表框中选择“宽带连接（默认）”选项，然后单击设置(S)按钮。

第3步：设置代理服务器

在打开的对话框中启用代理服务器，在“地址”文本框中输入“158.43.128.51”，在“端口”文本框中输入“3128”，然后输入用户名和密码，单击确定按钮完成代理服务器的设置。



2.4.4 禁止ping命令探测电脑

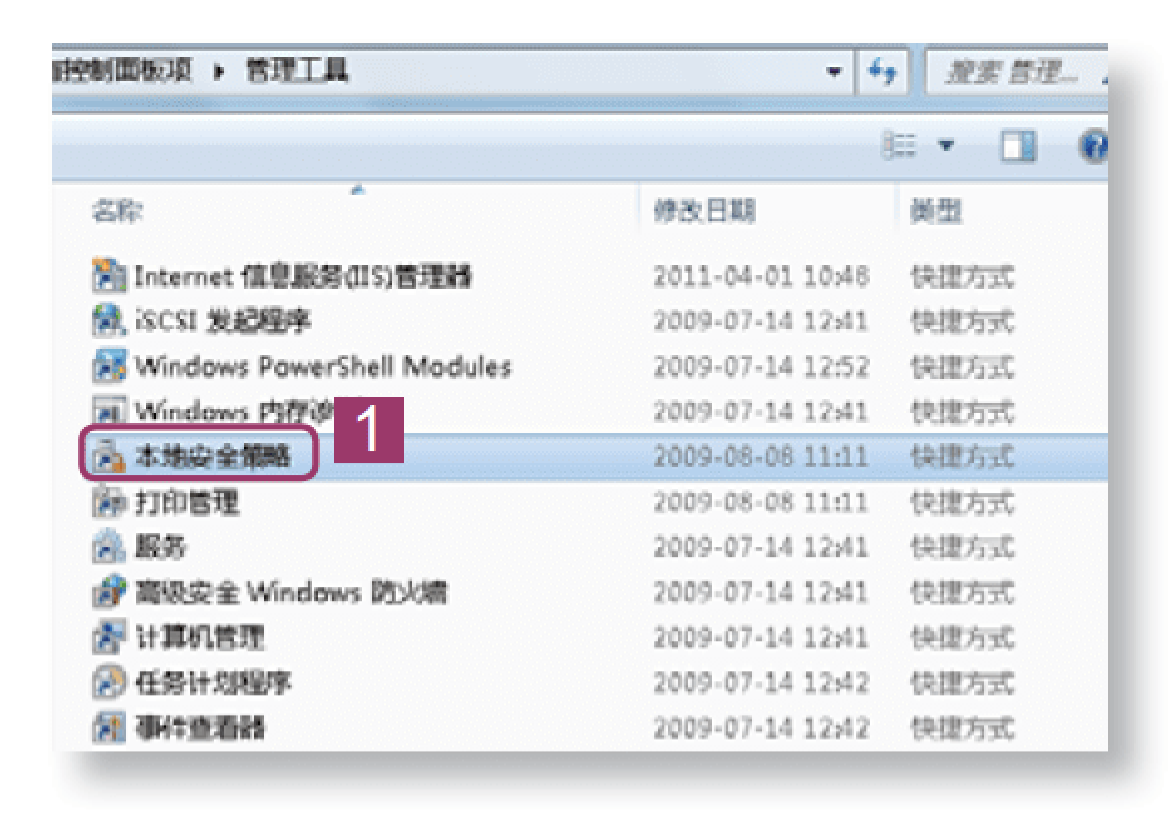
黑客在攻击电脑时，最常用的手段就是使用ping命令探测电脑的相关信息，为了阻止黑客的这种行为可通过设置IP安全策略禁止ping命令的使用。



下面将通过在本地安全策略中禁止使用ping命令来探测IP地址，其具体操作如下。

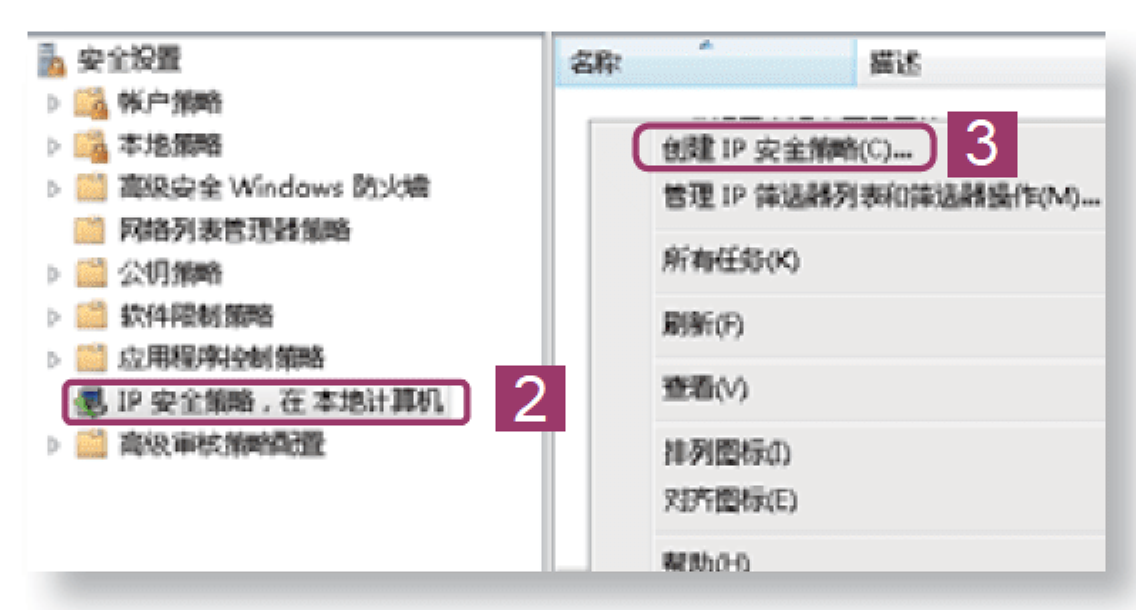
第1步：打开“本地安全策略”窗口

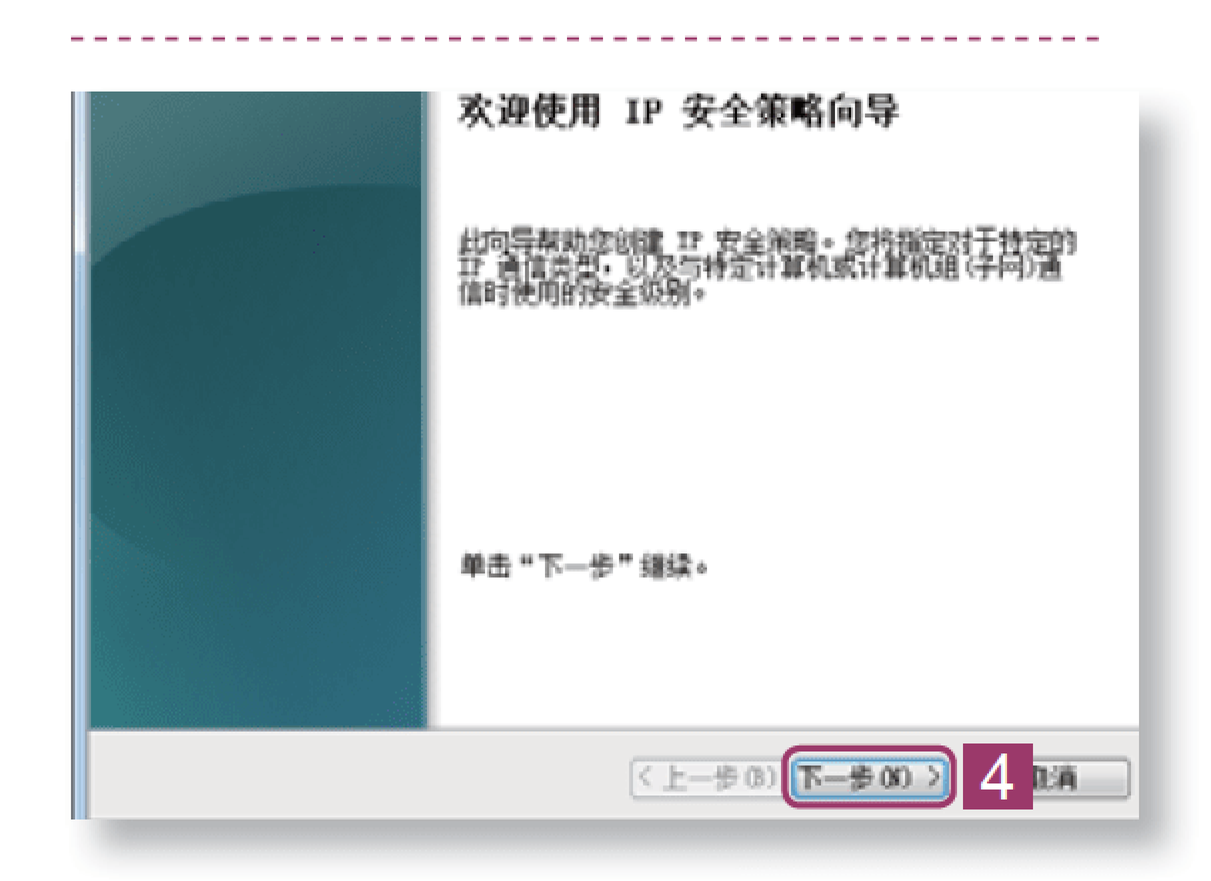
选择“开始”/“控制面板”命令，在打开的窗口中单击“管理工具”超链接，打开“管理工具”窗口，双击“本地安全策略”选项，即可打开“本地安全策略”窗口。



第2步：创建策略

在打开窗口的左侧窗格中选择“IP安全策略，在本地计算机”选项，在其右侧窗格中单击鼠标右键，在弹出的快捷菜单中选择“创建IP安全策略”命令。





第3步：打开IP安全策略向导

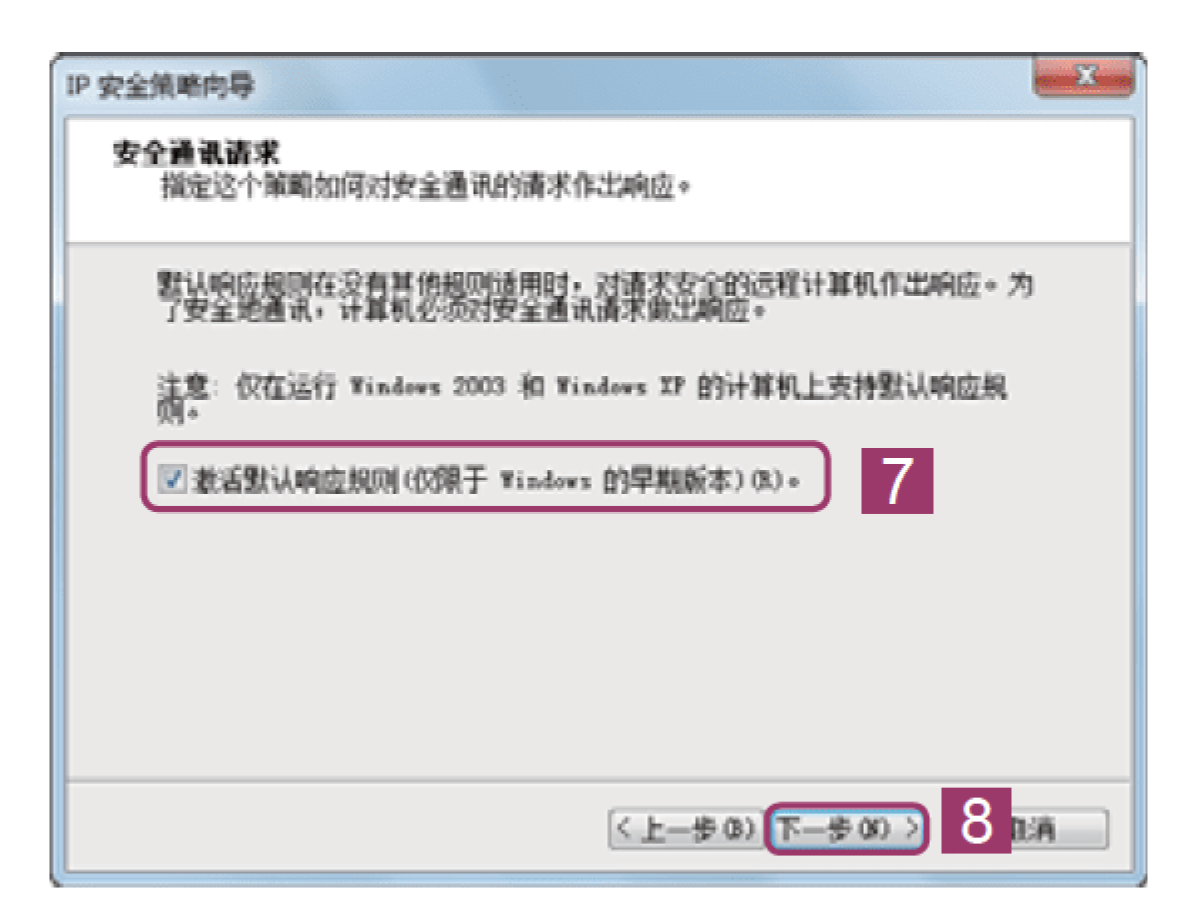
系统将打开“欢迎使用IP安全策略向导”界面，在其中将显示通过此向导可实现特定IP通信类型的安全级别，单击下一步(N) >按钮。



第4步：设置IP安全策略的名称

在打开“IP安全策略名称”界面的“名称”文本框中输入“禁止ping命令探测IP”，然后单击下一步(N) >按钮，打开“安全通信请求”对话框。





第5步：激活默认响应规则

在打开的对话框中选中“激活默认响应规则”复选框，然后依次单击下一步(N) >按钮直到完成规则的创建。

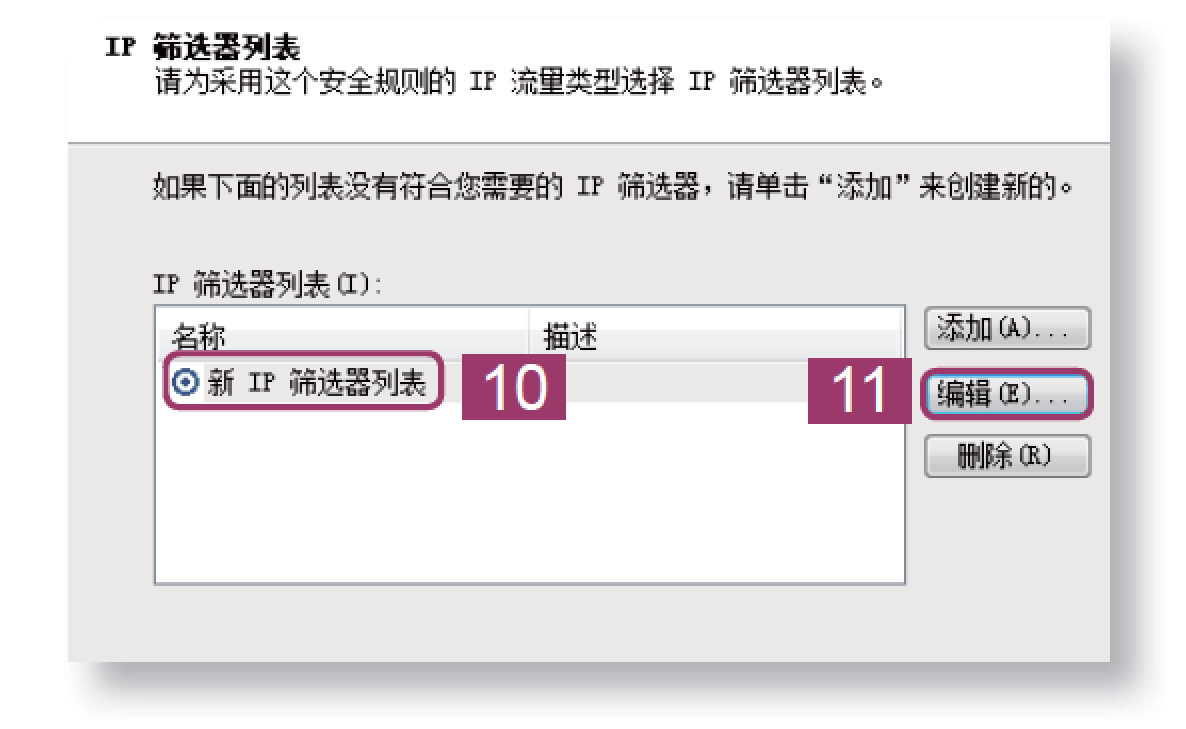
第6步：添加安全规则

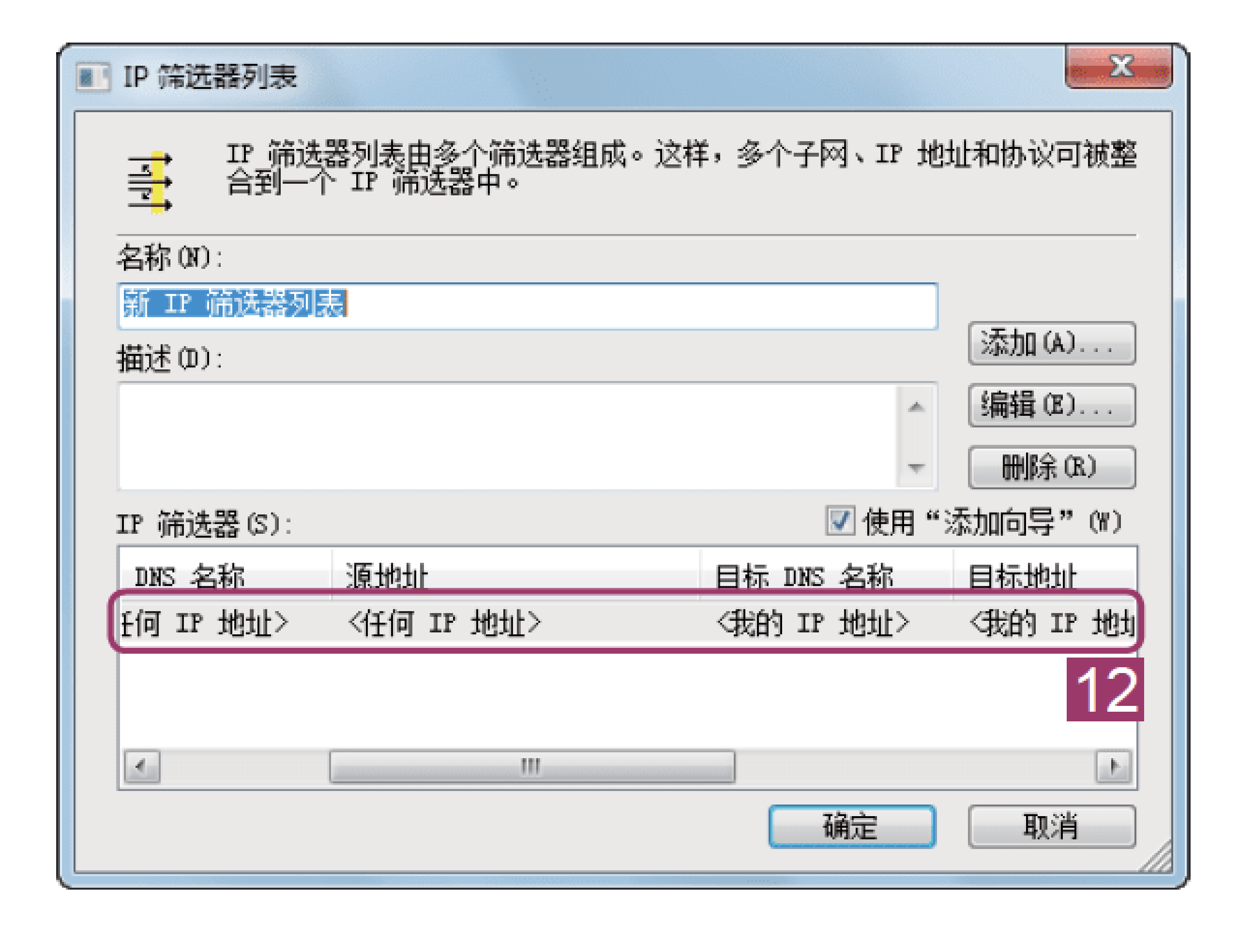
在打开的该规则属性对话框中单击添加(D)...按钮，打开“安全规则”向导，创建新的安全规则。



第7步：打开“IP筛选器列表”对话框

在打开的向导中依次单击下一步(N) >按钮，直到打开“IP筛选器列表”对话框，在其中选中“新IP筛选器列表”单选按钮，单击编辑(E)...按钮。





第8步：设置IP筛选器

在打开对话框的“IP筛选器”列表框中将其源DNS名称和源地址设置为“任何IP地址”，将目标DNS名称和目标地址设置为“我的IP地址”，将协议设置为ICMP，启用该IP规则即可。

提示：设置完成后，然后将其规则创建完成并启用该IP规则，即可实现禁止使用ping命令探测电脑的IP地址。

2.4.5 减少用户账户

在系统中不要设置太多的系统管理员账户，平时应使用一般用户权限登录系统，在需要安装软件或更改系统设置时再用系统管理员登录，这样会大大减少黑客破解管理员密码的机会。



下面将对在系统中删除用户账户的方法进行讲解，其具体操作如下。

第1步：打开“更改用户账户”窗口

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“用户账户”超链接，即可打开“更改用户账户”窗口，单击“管理其他账户”超链接。

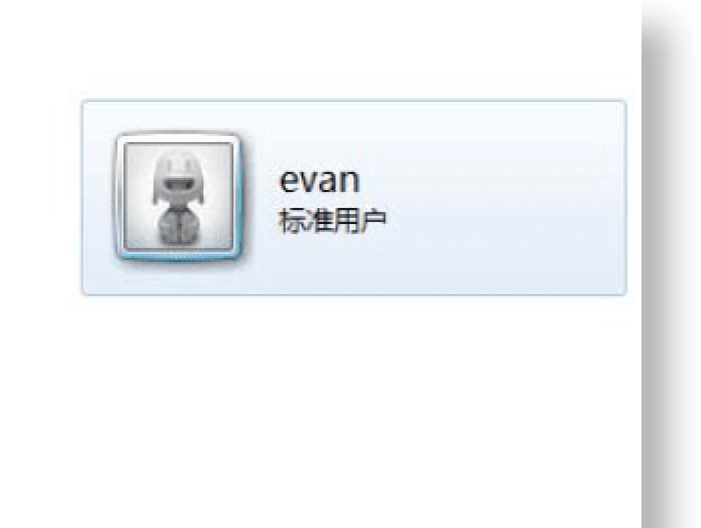




第2步：删除账户

在打开的对话框中选择“evan标准用户”选项，再在打开的“更改evan的账户”对话框中单击“删除账户”超链接将其删除。

提示：删除账户时，将打开提示窗口，询问是否删除相关文件，用户可选择保留文件或删除文件，也可取消删除操作。





2.4.6 防止黑客破坏网上交易

在进行网上交易时，一定要确认地址栏中的网址是要访问的网址。不要轻易透露银行账户和密码，否则会让黑客有机可趁，破坏网上交易，给用户造成损失。下面将对网上交易的几种安全措施进行讲解。

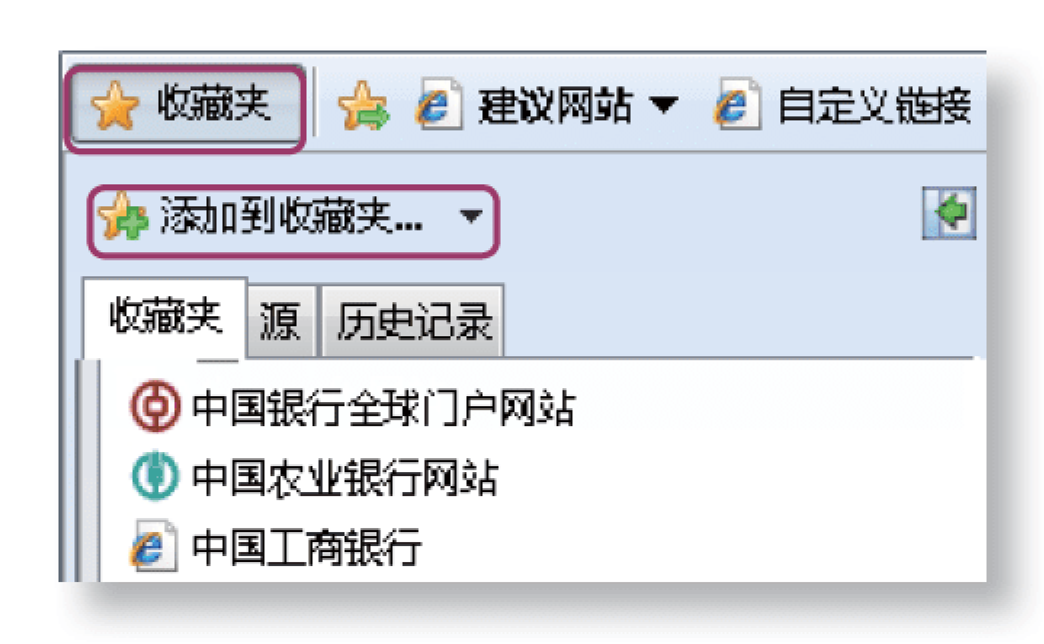
1. 避免进入钓鱼网站

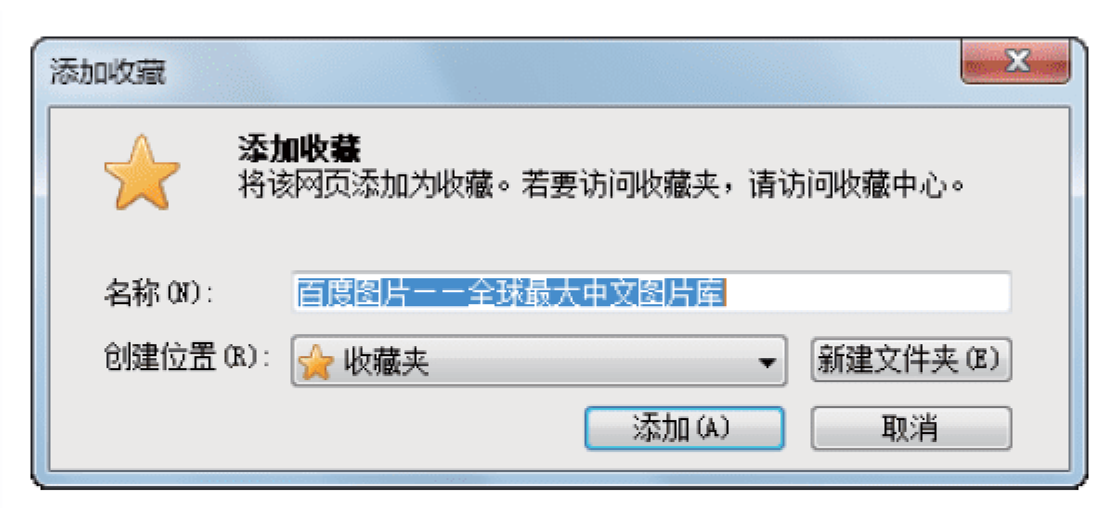
一些不法分子可能会在互联网上建立一些假网站，以诱使用户提供账号和密码，用户单击了网站中的链接，则可能在不知情的情况下安装木马程序或感染电脑病毒，使网上银行账号和密码被他人盗取。



要避免进入钓鱼网站，主要可通过如下几方面进行。

- **直接输入网址：**访问银行网站时直接输入网址登录，建议将银行网站地址添加到浏览器的“收藏夹”中，不采用超链接方式链接到银行网站。在浏览器中单击 收藏夹 按钮，再单击 添加到收藏夹... 按钮，打开“添加收藏”对话框，单击 确定 按钮即可对当前网站进行收藏。





- **识别虚假网站：**小心识别虚假的银行网站，若有任何怀疑，可以拨打银行服务热线。
- **对应证书信息：**用户在登录银行网站后，要仔细检查浏览器右下角状态栏上的挂锁图标对应的证书信息。

2. 安装网上银行安全插件

一些不法分子假冒银行网站或在线支付网页，诱使用户输入银行卡号、网上银行密码和口令等，盗取用户信息。

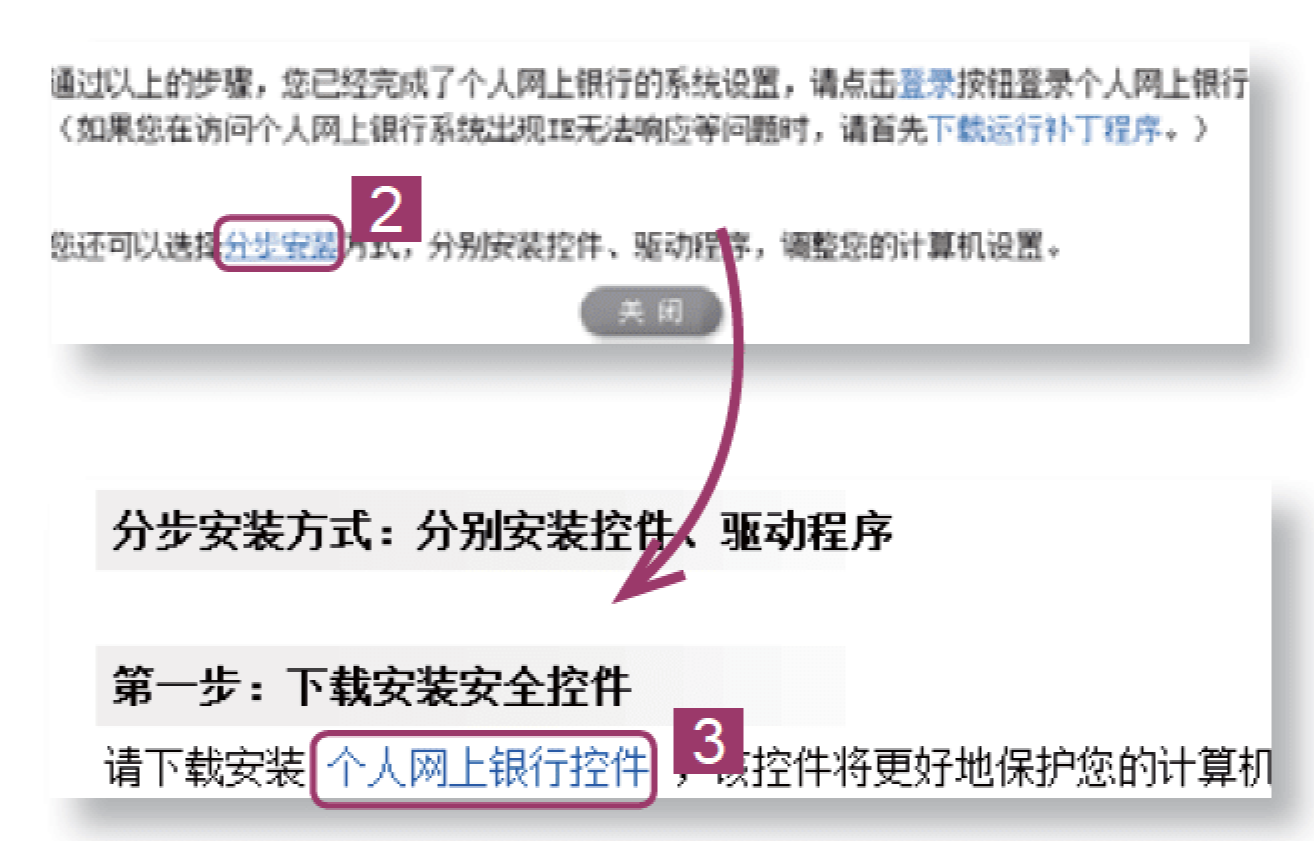


这里以中国工商银行为例讲解安装“防钓鱼”安全控件防范此类现象，其具体操作如下。

第1步：打开“安装”页面

打开中国工商银行网上银行首页（http://www.icbc.com.cn/icbc/），单击 个人网上银行登录 按钮下的“安装”超链接，找到控件所在位置。





第2步：下载安全控件

在打开的网页中单击“分步安装”超链接，在打开的安装步骤网页中单击“个人网上银行控件”超链接即可下载并安装安全控件。

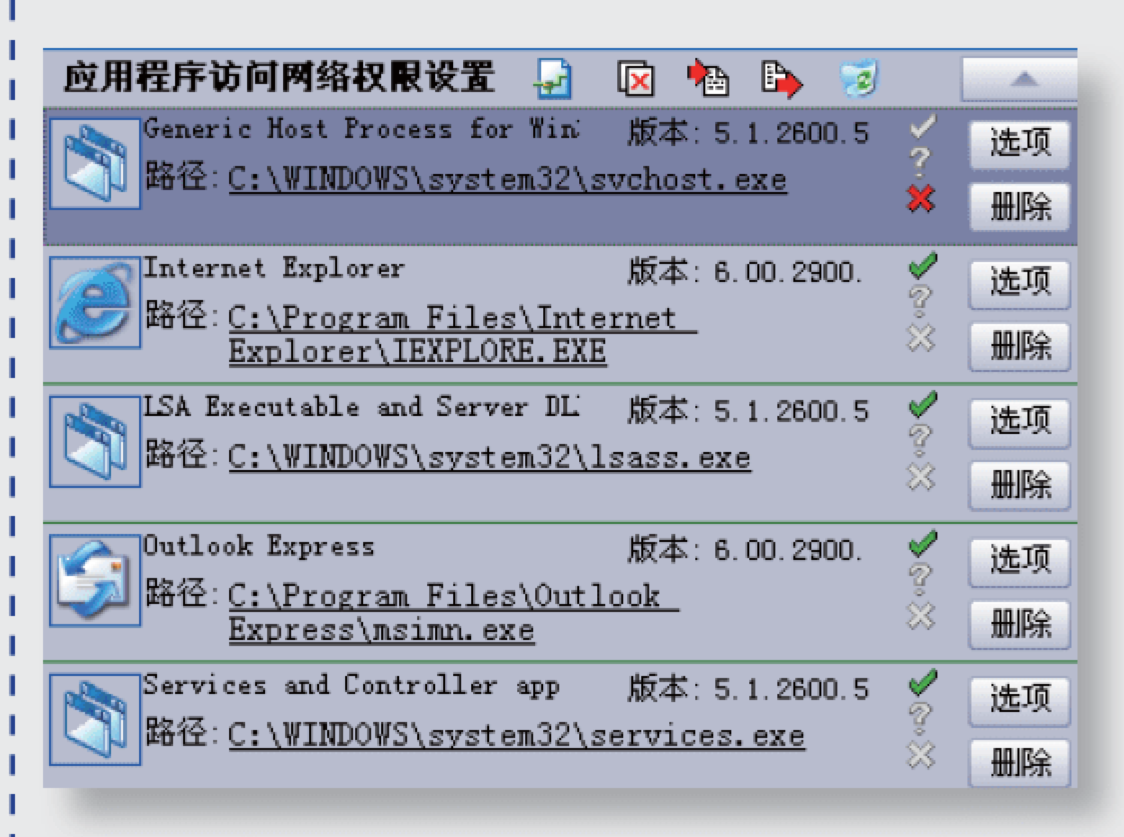
提示：在电脑中安装网上银行安全控件后，用户在进行网上交易时才不容易被不法分子窃取账号和密码，从而保障网上交易的安全。

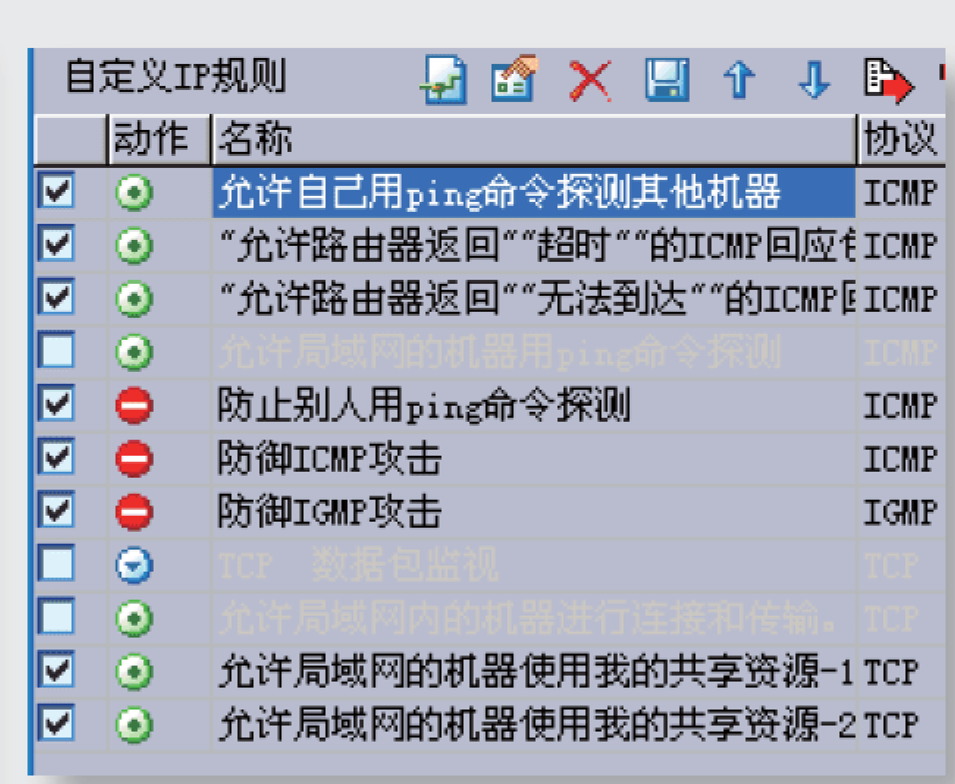
跟我练习

使用天网防火墙保护电脑的安全

任务1：电脑中有很多应用程序，为了防范黑客通过应用程序的漏洞对电脑进行攻击，使用天网防火墙设置应用程序访问网络的权限。

任务2：为了防止黑客通过网络协议对电脑进行攻击使用天网防火墙对IP规则进行设置。







2.5 更进一步——黑客常见攻击防范秘技

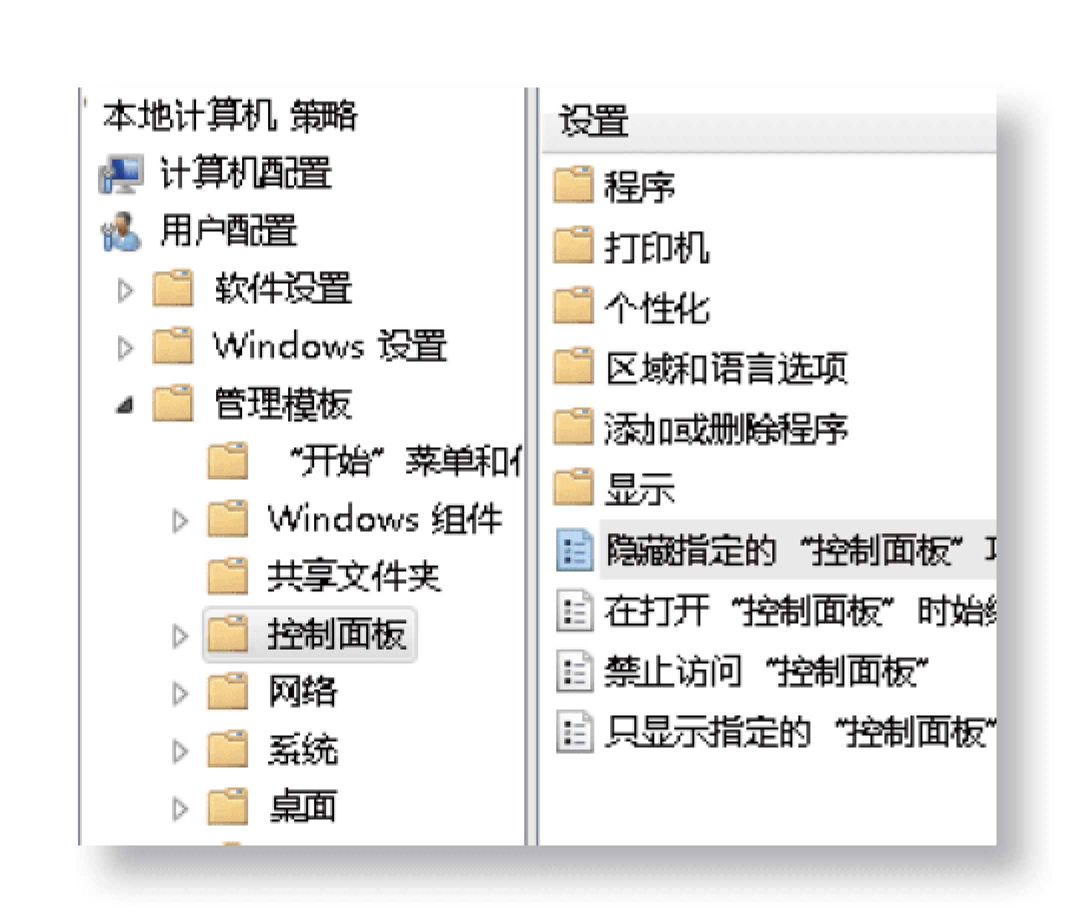
通过前面的学习，娜娜已经了解了黑客攻击的一般手段和攻击的方式，对黑客攻击也有了一定的认识，阿伟还教会了她如何来防止黑客的攻击，现在，阿伟还打算给她讲解几个关于防御黑客攻击的小技巧。

第1招 隐藏控制面板中的指定项目

控制面板中的“任务计划”和“游戏控制器”是黑客攻击电脑最常利用的途径，将其隐藏可有效避免黑客利用其进行攻击，其方法如下。

①选择“开始”/“运行”命令，然后执行gpedit.msc命令，启动组策略。

②在左侧窗格依次展开“用户配置/管理模板/控制面板”选项，在其右侧窗格双击“隐藏指定的‘控制面板’项”选项，在打开的对话框中选中“已启用”单选按钮，并设置要隐藏的对象，然后单击确定按钮即可。



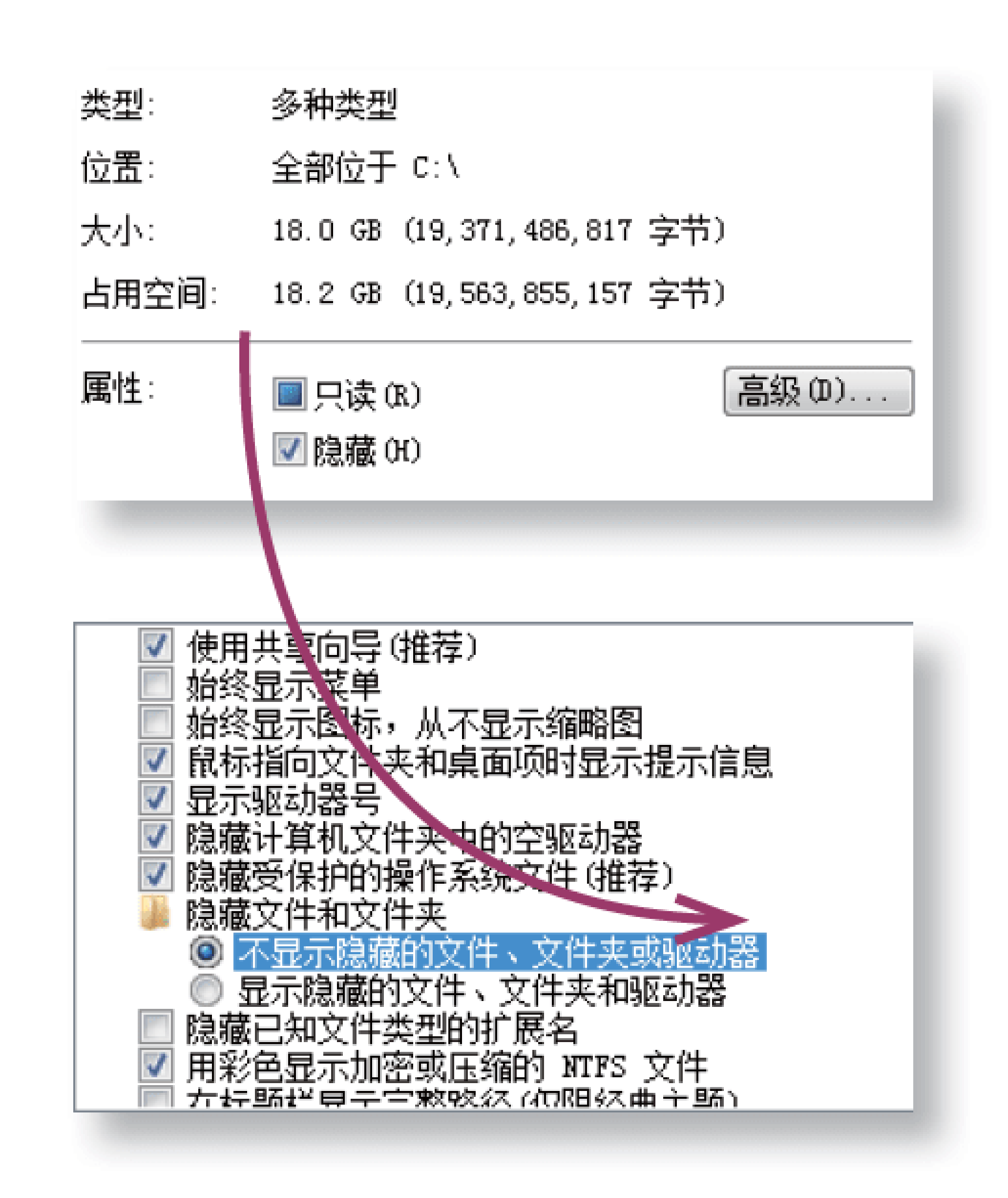
提示：选中“已启用”单选按钮后，可单击显示...按钮，在打开对话框的添加项目输入框中添加“任务计划”和“joy.cpl”，然后依次单击确定按钮可添加其他项目。

第2招 隐藏系统文件

在操作系统中可通过将系统文件进行隐藏以防止黑客及其他威胁破坏系统文件，其方法如下：

①在要隐藏的系统文件上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开的对话框中选中“隐藏”复选框，然后单击 确定 按钮。

②打开“计算机”窗口，选择“组织”/“文件夹和搜索选项”命令，打开“文件夹选项”对话框，选择“查看”选项卡，在其中选中“不显示隐藏的文件、文件夹或驱动器”单选按钮，单击 确定 按钮完成设置。



第3招 设置IE阻止弹出窗口

IE浏览器自带了弹出窗口的封堵功能，只要将它开启并进行必要的设置后，在使用其打开网页后就不会弹出烦人的广告类窗口，其方法如下：

①启动IE浏览器，然后选择“工具”/“Internet选项”命令，打开“Internet选项”对话框。

②在打开的对话框中选择“隐私”选项卡，在“弹出窗口阻止程序”栏中选中“启用弹出窗口阻止程序”复选框，然后单击 设置(E) 按钮。

③在打开对话框的“通知和阻止级别”栏中选中“阻止弹出窗口时播放声音”和“阻止弹出窗口时显示信息栏”复选框，然后单击 确定 按钮完成设置。





第4招 关闭文件和打印共享

文件和打印共享功能是黑客入侵很好的安全漏洞。因此，在没有必要使用"文件和打印共享"功能的情况下可以将其关闭，其方法如下：

①在"网络"图标上单击鼠标右键，在弹出的快捷菜单中选择"属性"命令，打开"网络和共享中心"窗口。

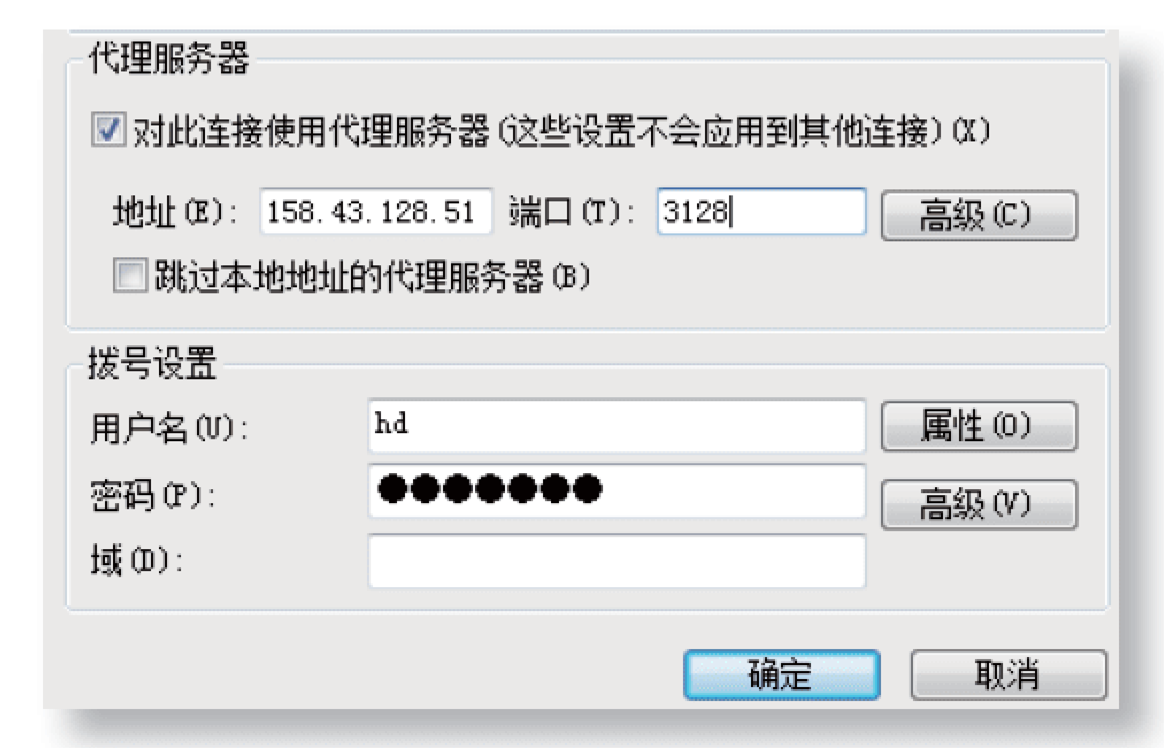
②在打开的窗口中单击"更改高级共享设置"超链接，在打开的窗口中选中"关闭文件和打印机共享"和"关闭公用文件夹共享"单选按钮，然后单击保存修改按钮完成设置。



2.6 活 学 活 用

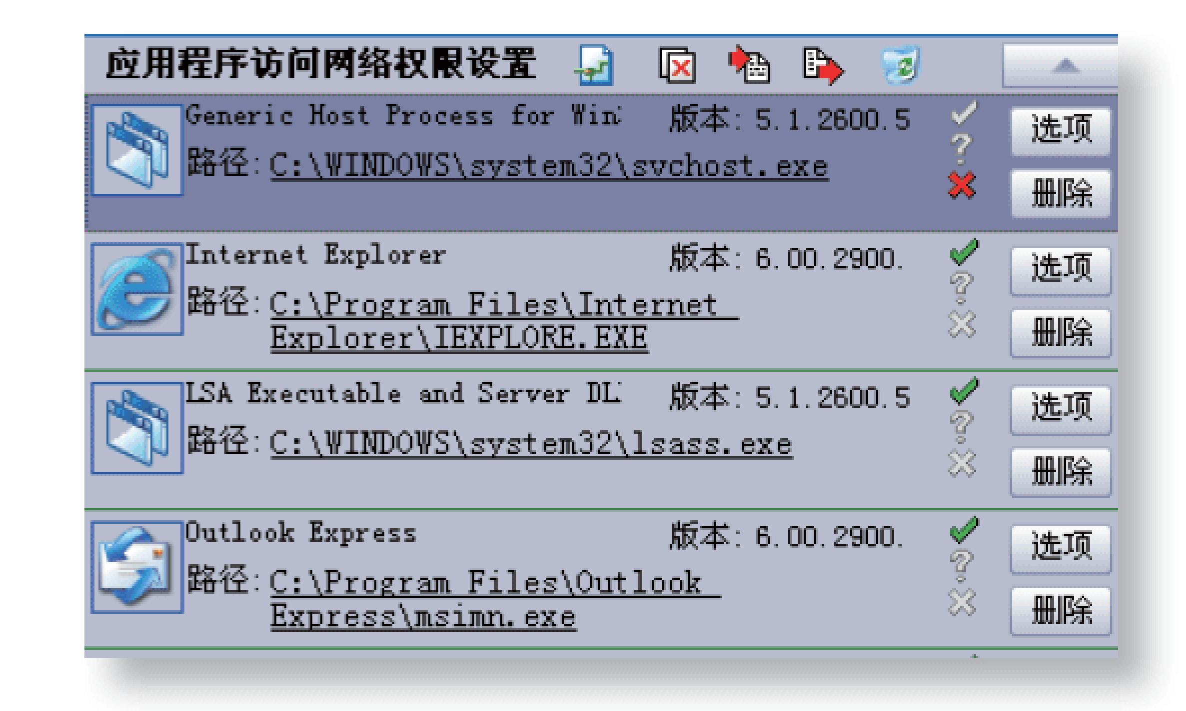
（1）了解什么是黑客，并简述黑客攻击电脑的目的和基本准则，查阅相关资料了解黑客攻击电脑的一般手段。

（2）在相关网站获得代理服务器的IP地址和端口号，并通过设置使用代理服务器达到隐藏本地IP地址的目的。



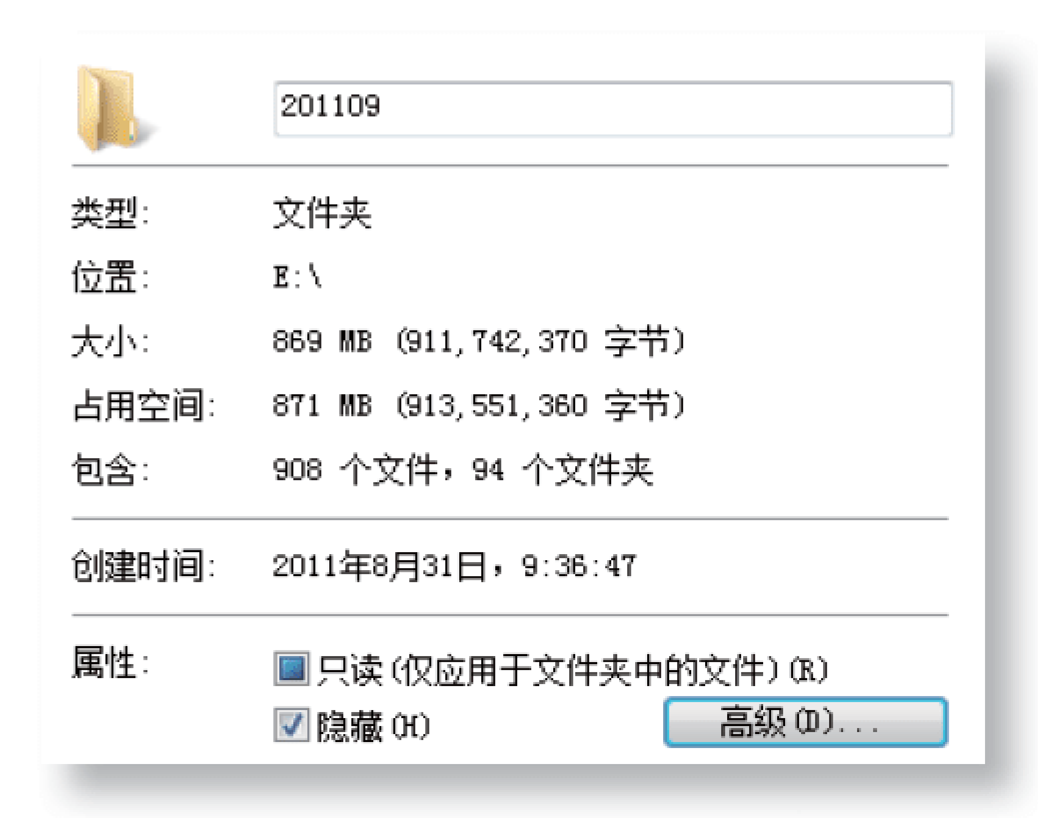
提示：用户可在免费代理服务器的网站中找到免费的代理服务器，也可以用代理猎手等工具进行查找。

（3）搜索并下载天网防火墙，然后在电脑中进行安装，安装完成后对其相应的IP规则进行设置，使黑客无法通过IP的漏洞攻击电脑。



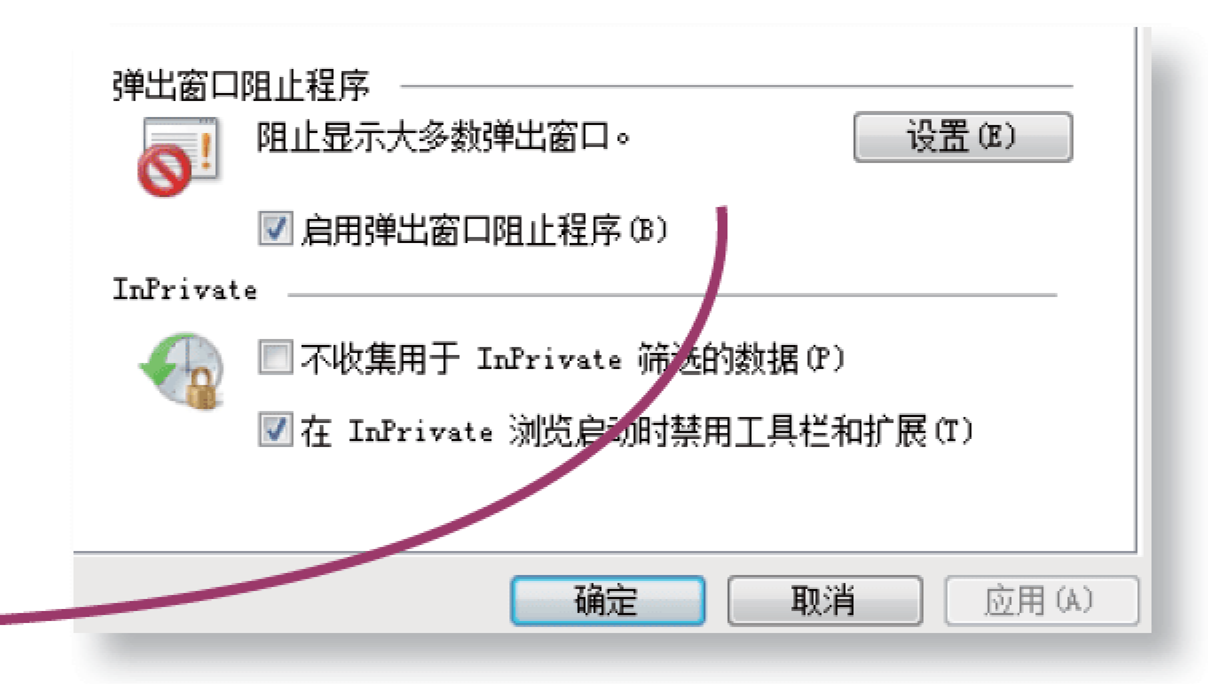
（4）将电脑中的重要资料进行隐藏，避免被黑客窃取。

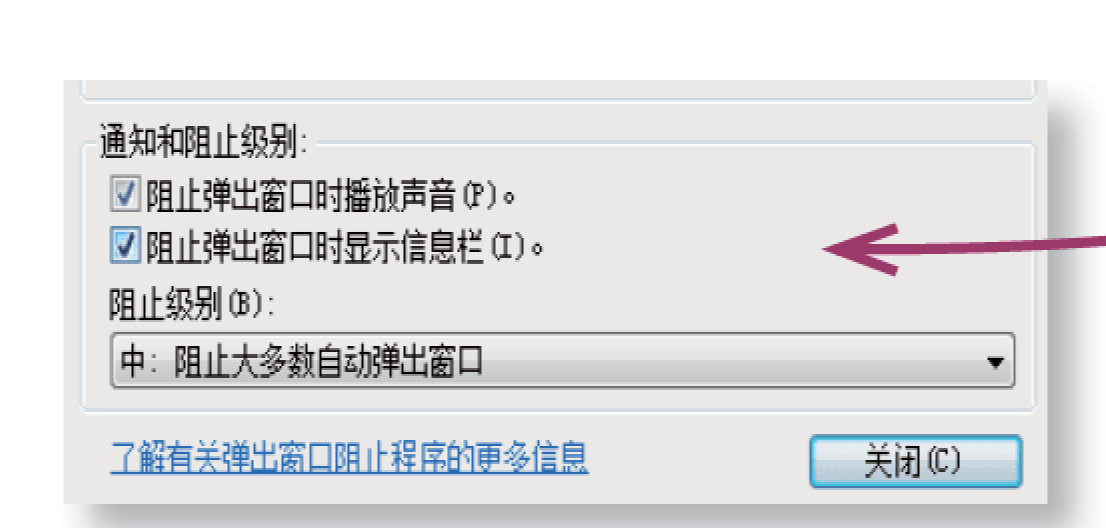
提示：包括设置文件自身的属性和“文件夹选项”对话框中“查看”选项卡的相关选项。



（5）在网上下载使用网上银行交易的安全权证书进行安装，并在输入网址进入相关网页时确认输入的地址是否正确。

（6）设置IE浏览器阻止弹出窗口，防止进入恶意网站使黑客有机可趁。







- ☑ 想知道病毒和木马的区别吗？
- ☑ 还在为不知道怎样辨别木马和病毒而烦恼吗？
- ☑ 想知道怎样来预防电脑感染病毒和木马吗？
- ☑ 想知道怎样使用杀毒软件查杀病毒吗？



第 03 章 拒绝病毒和木马的入侵

娜娜的电脑今天用起来速度很慢，并且有时候鼠标还“不听指挥”，这可把她急坏了，因为她还有很多的任务需要完成，但速度却始终上不来。这时，她想到了阿伟，决定让阿伟给她看看到底是哪里出问题了，阿伟一看她的电脑，就知道是中病毒了，帮她弄了半天，终于解决了这些问题，娜娜此时迷惑了，“为什么阿伟知道她电脑感染了病毒呢？”带着这个问题，她决定去请教阿伟。

3.1 揭秘病毒和木马

阿伟告诉娜娜：“木马和病毒对电脑的危害巨大，要完全防范病毒和木马是不可能的，只能根据病毒和木马的特征，做出相应的防范措施。”说到这里，娜娜问阿伟：“那我应该怎样做才能有效预防病毒和木马的感染呢？”接下来阿伟便开始讲解。

新手解惑

Q：病毒和木马有什么区别和联系？

A：木马是病毒的一种，它是一种远程控制类病毒，一般都是黑客用来控制用户电脑的病毒。病毒的意义就要广泛多了，包括木马、广告间谍以及恶意破坏文件系统的程序等。

3.1.1 病毒和木马的特征

电脑在感染病毒或木马后并不会马上出现症状，一般不容易察觉到，但是当其发作时往往是致命的，这也是其鲜明特征的表现。



下面将分别介绍病毒和木马的特征。

1. 病毒的特征

病毒相对于其他软件有其独有的特征，下面将分别进行介绍。

- **可执行性：** 病毒与其他合法程序一样是一段可执行程序，但它寄生在其他可执行程序上。
- **传染性：** 病毒也会通过各种渠道从已被感染的电脑扩散到未被感染的电脑，将可能造成被感染的电脑工作失常甚至瘫痪。
- **破坏性：** 病毒的破坏性主要取决于病毒设计者的目的，有的破坏性非常大，会损坏文件、系统，有的则小很多。
- **潜伏性：** 潜伏性是指病毒程序需使用专用检测程序进行检查或病毒需要一定的条件进行激发。
- **隐蔽性：** 由于电脑的隐蔽性，病毒可在用户没有察觉的情况下扩散并游荡于网络中无数电脑之间。
- **针对性：** 病毒一般都是针对于特定的操作系统和特定的应用程序进行传播的。



■ **可触发性**：病毒因某个事件或数值的出现，诱使其实施感染或进行攻击的特性称为可触发性。它的触发机制就是用来控制感染和破坏动作频率的。

2. 木马的特征

木马可以看作是一个间谍，不管它有什么功能，有什么“居心”，它总是听命于自己的“主人”，一发现什么组织兴趣的东西，就会想方设法汇报。 因此，可将木马看成一个以窃取情报为目的，并想尽一切办法逃避杀毒软件追捕的间谍。

3.1.2 如何发现病毒和木马

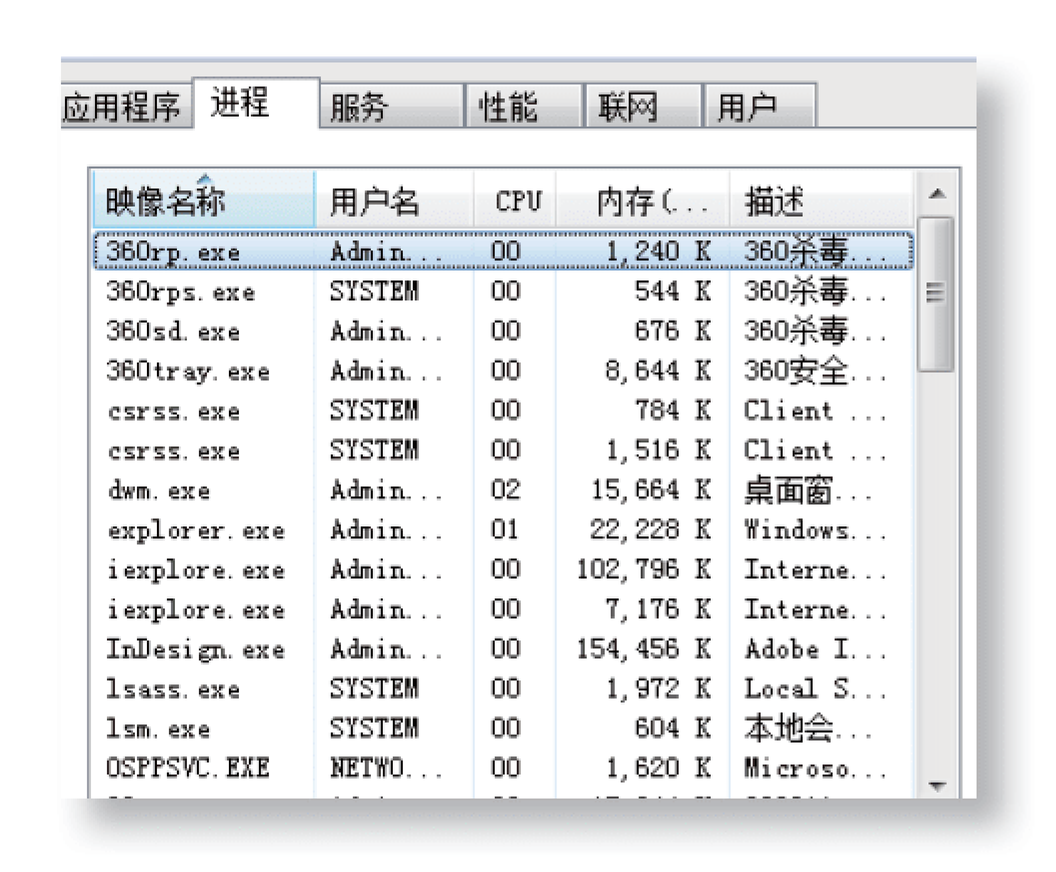
电脑感染病毒或木马后，如及时发现，即使我们不能马上将其全部清除，也可将损失尽量降低。



在电脑中，应该怎样来辨别病毒和木马呢？最简单的方法是通过查看进程和电脑表现的异常情况进行病毒和木马的判断，下面将分别进行介绍。

1. 通过查看系统进程发现

在Windows 7操作系统中，按Ctrl+Alt+Delete键，启动任务管理器，在“进程”选项卡的列表框中即可查看系统中的进程，判断其病毒与木马的存在与否。



新手解惑

Q：什么是进程？怎样通过进程来判断系统是否存在病毒？

A：操作系统当前正在运行的程序就是进程，主要包括操作系统管理电脑和完成各种操作所需要的程序以及用户开启、执行的额外程序等。某些病毒会以“进程”的形式出现在系统中，通过打开系统进程列表来查看哪些进程正在运行，通过进程名及路径判断是否有病毒。

电脑的进程主要分为基本系统进程和附加进程两类，基本系统进程对电脑的正常运行起着至关重要的作用，不能随便将其结束。

基本系统进程

名　　称	作　　用
Csrss.exe	负责控制Windows创建或删除线程以及16位的虚拟DOS环境
Lsass.exe	管理IP安全策略以及启动ISAKMP/Oakley（IKE）和IP安全驱动程序
Explorer.exe	显示系统桌面上的图标以及任务栏图标
Smss.exe	负责启动用户会话
Servi.exe	系统服务的管理工具，包含很多系统服务
System	Windows系统进程
System Idle Process	作为单线程运行的，并在系统不处理其他线程时分派处理器的时间
Spoolsv.exe	管理缓冲区中的打印和传真作业
Svchost.exe	创建需要加载的服务列表
Winlogon.exe	管理用户登录系统

提示：除了基本系统进程之外，还有附加进程，附加进程可以随意结束，不会影响系统的正常运行。

2. 根据系统表现的症状判断

当电脑出现一些异常现象，就应该使用杀毒软件进行扫描，确认是否中毒，病毒和木马入侵和潜伏的过程并不是完全毫无踪迹。其表现的异常包括如下几方面。

- 启动速度变慢：启动电脑后，在一段时间内系统对用户的操作无响应或响应变慢。
- 资源消耗加剧：硬盘中的存储空间急剧减少，系统中基本内存发生变化，CPU经常保持高使用率。
- 文件丢失或被破坏：电脑中的文件莫名丢失、文件图标被更换、文件的大小和名称被修改、文件内容变成乱码，文件无法打开。
- 性能下降：电脑运行程序时经常提示内存不足或出现错误；电脑经常在没有任何征兆的情况下突然死机；硬盘经常出现不明的读写操作，在未运行任何程序时，硬盘指示灯不断闪烁甚至长亮不熄。

提示：除此之外，还可根据系统的时间和日期无故发生变化，自动打开IE浏览器链接到不明网站，出现莫名其妙的画面和提示以及电脑的输入/输出端口不能正常使用等进行判断。



3.1.3 怎样预防病毒和木马

在电脑的使用过程中，通常我们关心的是如何将病毒拒之门外，与其等到电脑感染病毒后再进行查杀，不如先做好必要的防范措施，让病毒无“用武之地”。



下面将介绍预防病毒和木马的方法。

1. 预防病毒

病毒固然猖獗，它能对电脑造成严重的威胁，但只要用户加强病毒防范意识和防范措施，就可以降低电脑被病毒感染的几率和破坏的程度。电脑病毒的预防主要包括如下几方面。

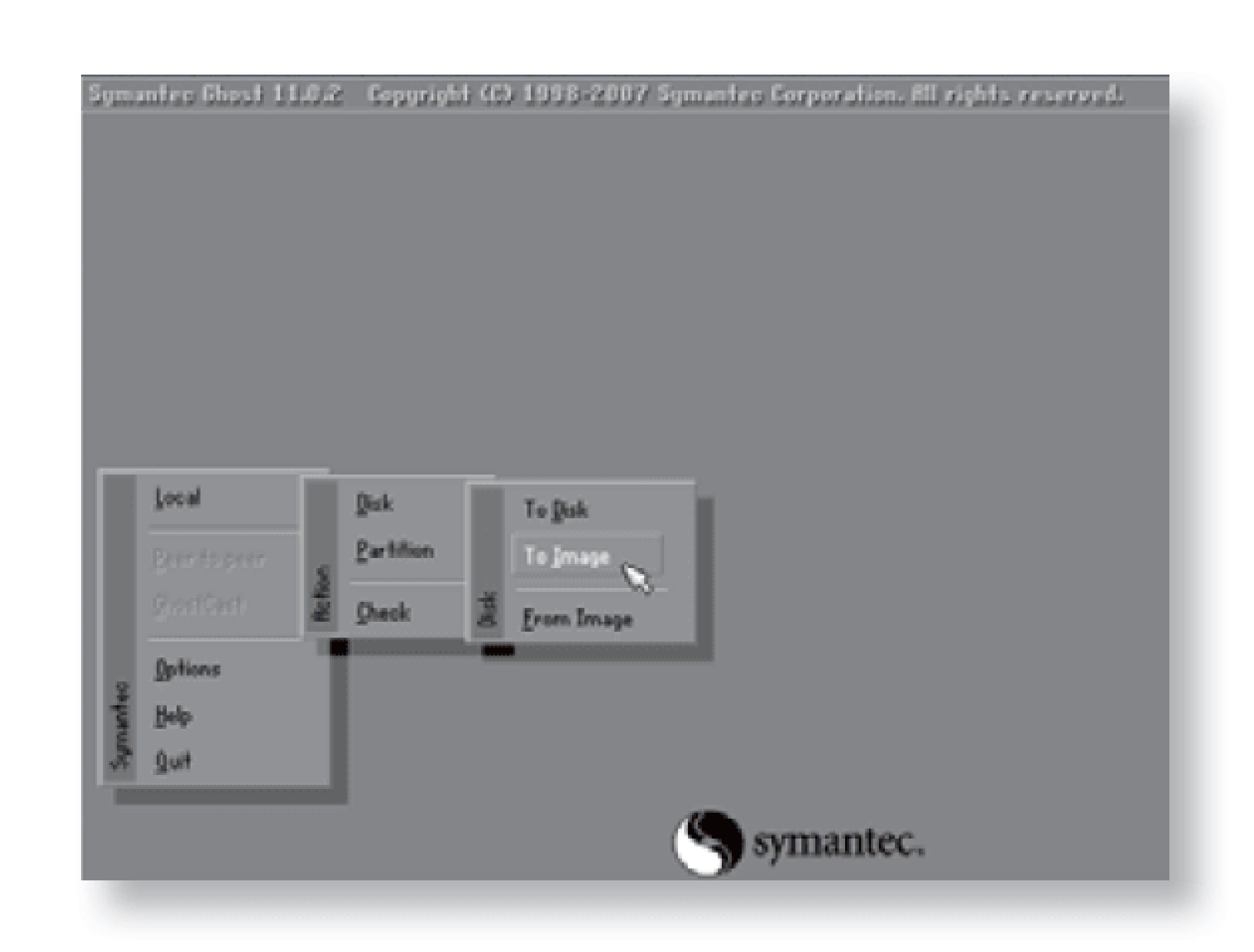


方法1：安装杀毒软件

说明：在电脑中安装杀毒软件，开启软件的实时监控功能，并定期升级杀毒软件的病毒库，这样将及时地针对病毒进行拦截并做出相应的处理，有效预防病毒感染电脑。

方法2：备份重要数据

说明：在电脑中使用备份工具软件（MaxDOX）备份操作系统，可在电脑中毒后利用备份进行及时恢复。同时，重要数据和文件应利用移动存储设备或光盘备份，这样可以减少病毒造成的损失。



提示：另外，还可以通过使用正版软件，不使用盗版和来历不明的软件；网上下载的文件要先杀毒再打开；使用移动存储设备时也应先杀毒再使用；学习最新病毒的防治和处理等方法进行预防病毒的感染。

2. 预防木马

木马制造者不断地编写新的木马，随着网络的普及，这些木马的传播速度越来越快，且新的变种层出不穷，在检测、清除的同时，更要注意采取措施来预防。预防木马的方法主要包括以下几个方面。

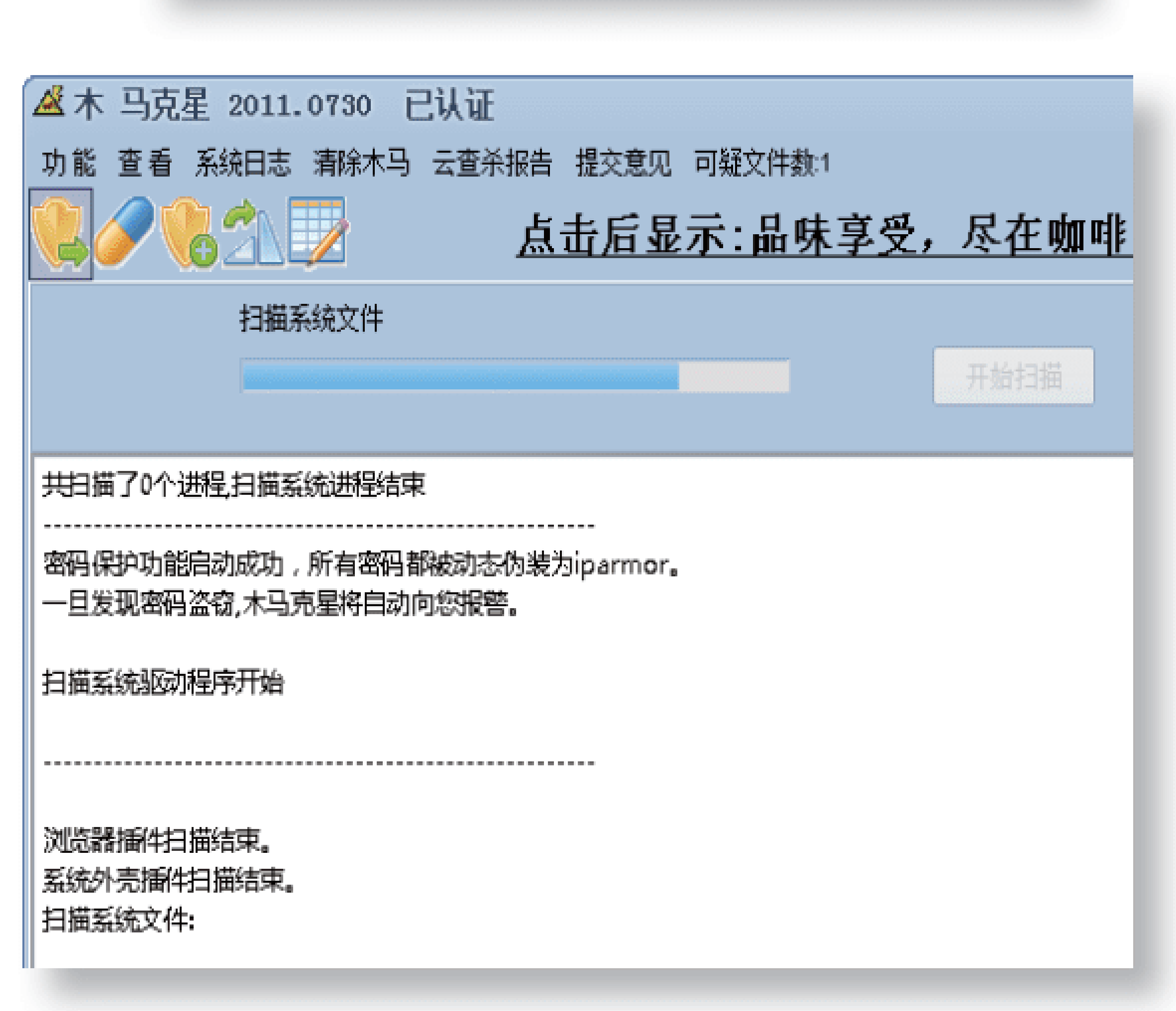
方法1：始终显示文件扩展名

说明：在电脑中可以将Windows资源管理器配置成始终显示文件扩展名，扩展名为vbs、shs、pif的文件多为木马的特征文件，如果查看到这些可疑的文件扩展名时就应该引起注意，及时作出处理。

文件夹视图
可以将该文件夹正在使用的视图(例如“详细信息”或“图标”)应用到所有这种类型的文件夹中。
应用到文件夹(L)　重置文件夹(R)
高级设置:
鼠标指向文件夹和桌面项时显示提示信息
显示驱动器号
隐藏计算机文件夹中的空驱动器
隐藏受保护的操作系统文件(推荐)
隐藏文件和文件夹
不显示隐藏的文件、文件夹或驱动器
显示隐藏的文件、文件夹和驱动器
隐藏已知文件类型的扩展名
用彩色显示加密或压缩的 NTFS 文件
在标题栏显示完整路径(仅限经典主题)
在单独的进程中打开文件夹窗口
在缩略图上显示文件图标
还原为默认值(D)

方法2：运行木马实时监控程序

说明：如果正在使用的电脑已联入互联网，则应运行反木马实时监控程序，绝大多数监控软件都能实时显示当前所有运行程序并有详细的描述信息，这里推荐木马克星，它能有效地检测木马的存在与否。



方法3：不要执行来历不明的软件

说明：木马一般绑定在其他软件中，一旦用户运行了该软件将被感染，因此应在安全性较高的站点进行软件的下载，并且在软件安装之前需用反病毒软件检查，确定无毒后再运行。

方法4：不要随意打开邮件附件

说明：现在绝大部分木马都是通过邮件来传递的，而且有的还会连环扩散，因此对邮件附件的运行尤其需要注意。

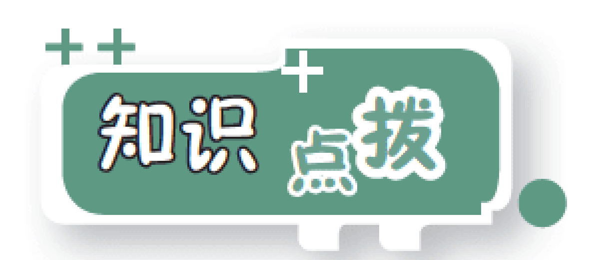


3.2 反病毒木马软件的应用

阿伟在讲解病毒和木马的基本知识时，娜娜注意到了在此过程中经常提到杀毒软件的使用，娜娜对此很疑惑，因为她电脑中使用的杀毒软件都是别人帮她安装的，她也从来没使用过，听了阿伟的介绍，她意识到了杀毒软件的重要性，于是要求阿伟为她讲解有关毒软件的知识。

3.2.1 常见杀毒软件简介

目前，电脑病毒非常泛滥，反病毒软件成为了对付病毒的有力武器，目前的杀毒软件种类也很多，可供用户选择使用。



下面介绍几款功能较全、应用较广泛的杀毒软件，用户可根据需要进行选择。

1. 卡巴斯基杀毒软件

卡巴斯基杀毒软件是一款优秀的网络杀毒软件，查杀病毒性能远高于同类产品。这种杀毒软件具有超强的中心管理和杀毒能力，且提供了所有类型的抗病毒防护、抗病毒扫描仪、监控器、行为阻段和完全检验功能。





2. 江民杀毒软件

江民杀毒软件KV2011是全功能专业安全软件，全面融合杀毒软件、防火墙、安全检测、漏洞修复等核心安全功能为一个有机整体，打破杀毒软件、防火墙等专业软件各司其职的界限，为个人电脑用户提供全面的安全防护。



3. 360杀毒软件

360杀毒和360安全卫士是360安全中心出品的一款免费的云安全软件。360杀毒具有查杀率高、资源占用少、升级迅速等优点。同时，360杀毒可以与其他杀毒软件共存，是一个理想杀毒备选方案。360安全卫士中集成有木马防火墙，能有效防御木马的入侵。

4. 金山毒霸

金山毒霸在查杀病毒种类、查杀病毒速度、未知病毒防治等多方面达到先进水平，同时金山毒霸具有病毒防火墙实时监控、压缩文件查毒、查杀电子邮件病毒等多项先进的功能。紧随世界反病毒技术的发展，为个人用户和企事业单位提供完善的反病毒解决方案。



3.2.2 360杀毒软件的应用

娜娜的电脑装有360杀毒软件，这款软件是目前使用最广泛的反病毒软件之一，且操作简单，特别适合初学者进行使用。

1. 查杀指定位置的病毒程序

使用360杀毒软件查杀电脑指定位置的病毒程序能为用户节约杀毒时间，并能够根据用户的判断准确地进行查杀病毒。





下面将使用360杀毒软件扫描电脑C盘，检测其是否存在病毒，并对扫描到的病毒程序进行处理，其具体操作如下。



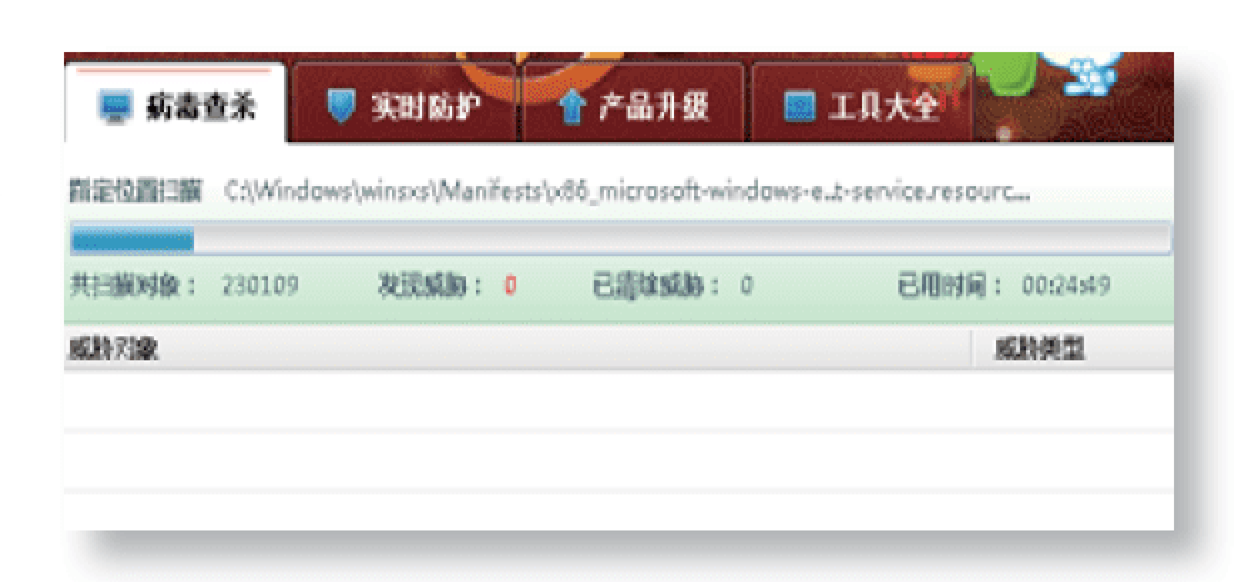
第1步：选择扫描对象

启动360杀毒软件，在其主界面上单击按钮，选择“指定位置扫描”方式，在打开的对话框中选择“本地磁盘（C:）”选项，然后单击扫描按钮。



第2步：扫描病毒

系统开始扫描，在此过程中用户可暂停或结束扫描，扫描完成后，如发现可疑程序，系统将提醒用户进行相应处理。



教你一招

使用360杀毒软件进行全盘查杀

启动360杀毒软件，在其中选择全盘扫描功能，系统将开始对整个磁盘进行扫描，全面查杀电脑中的病毒程序，防止病毒破坏电脑。

2. 开启实时防护功能

在电脑中开启360实时防护功能能有效地防止病毒的入侵，阻止其破坏电脑，使电脑处于一个安全的状态。



下面将开启360实时防护功能，并设置其安全级别，其具体操作如下。



第1步：开启防护功能

启动360杀毒软件，选择“实时防护”选项卡，然后在其中单击一键打开按钮即可开启其防护功能。



第2步：打开“设置”对话框

在“实时防护”选项卡右侧窗格中可查看防护的信息，单击“设置”超链接即可打开“设置”对话框。

第3步：设置实时防护

在打开的对话框中拖动滑块，将其设置为中级安全级别，然后在“监控的文件类型”栏中选中“仅监控程序及文档文件”单选按钮，在“其他防护选项”栏中选中全部复选框，最后单击确定按钮。



3.2.3　360木马防火墙的应用

除了360杀毒软件外，360安全中心还为用户提供了木马防护工具——360木马防火墙，在电脑中开启360木马防火墙能有效拦截木马，还系统一片清净。





要设置360木马防火墙，首先需确定电脑已安装360安全卫士，在360安全卫士中启动其设置窗口，再对其进行相应设置即可。

第1步：开启360木马防火墙

启动360安全卫士，选择“功能大全”选项卡，单击“360安全产品”栏中的“360木马防火墙”按钮，打开360木马防火墙。





第2步：开启木马防火墙

在打开的360木马防火墙界面中单击一键开启按钮开启其保护功能，然后选择“设置”选项卡，进入木马防护墙设置界面。

提示：在其中选择“信任列表”和“阻止列表”选项卡，可在其界面中添加相应的选项。

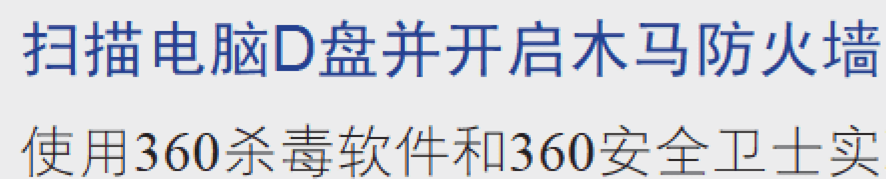


第3步：设置木马防火墙

在打开的对话框中选择“系统防御”选项卡，并在右侧的界面中选中“智能模式”单选按钮，然后再选中其中的所有复选框，单击保存按钮保存设置。

提示：在360木马防火墙右侧显示了弹窗模式、防御历史和信任/阻止列表等内容，用户可单击其相应的“查看详情”超链接切换到相应界面，在“弹窗模式”栏中单击右侧的“更改设置”超链接可对设置进行更改。

跟我练习



扫描电脑D盘并开启木马防火墙

使用360杀毒软件和360安全卫士实现电脑的杀毒及预防木马的入侵。

任务1：使用360杀毒软件的指定位置扫描功能对电脑的D盘进行扫描，并对扫描的结果进行处理。

任务2：在360安全卫士中开启木马防火墙，设置相关的防御方式。



3.3 遭遇新病毒该怎么办

通过阿伟对杀毒软件使用方法的讲解，娜娜终于知道怎样使用杀毒软件对自己的电脑进行防护并扫描电脑病毒了，但是在进行病毒查杀时，娜娜发现有病毒程序始终清除不了，这时，她又找到了阿伟。阿伟告诉她：“这可能是一种新型的病毒，让我来教你怎样解决它。”

3.3.1 对未知病毒的查找和分析

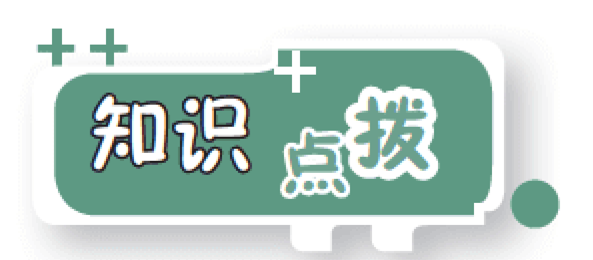
如果在你的电脑中发现异常但使用杀毒软件又检测不到病毒时，这时可使用杀毒软件的可疑文件扫描功能扫描系统中可能存在的威胁文件。

查找到新病毒后可根据列表中显示的文件名及路径去查找被感染文件，用户可将其删除，也可以提交给反病毒中心进行分析，然后根据分析再进行处理。



3.3.2 新型病毒处理

如果出现了一种新型病毒，通常杀毒软件制造商就会推出专门查杀该病毒的专杀工具。用户可先了解关于该病毒及其变种的说明和症状表现形式，判断自己的电脑是否感染了该病毒，再在相应杀毒软件官方网站中查找并下载其专杀工具对电脑进行全面扫描。



下面将介绍几种新型病毒及处理方法。

1. QQ群蠕虫病毒

电脑中此病毒会自动访问QQ群共享空间进行传播。该病毒主要目的是盗取魔兽世界、常见电子邮箱和社交网络的账户密码，以“成人电视棒升级破解版”为名诱骗网民下载运行。

目前，金山毒霸已经与腾讯安全部门进行紧急磋商，且金山毒霸与QQ电脑管家已经可完美拦截。





2. 机器狗病毒

最新版本的机器狗病毒入侵成功后，会自动下载大量木马、病毒、恶意软件、插件等，几乎所有安全软件均不能正常使用，大量用户也因此而不得不选择重装系统。

使用瑞星专用清除工具可准确地检测出此类病毒，并将其彻底清除，以保护电脑的安全。



3. AV终结者

电脑中了该病毒后，会出现禁用所有杀毒软件以及相关安全工具，让用户电脑失去安全保障；破坏安全模式；强行关闭带有病毒字样的网页；在各磁盘根目录创建可自动运行的exe程序和autorun.inf文件，一般用户重装系统后，会习惯性地双击硬盘分区盘符打开硬盘，病毒将再次被运行。



4. 新鬼影病毒

新鬼影病毒主要通过假冒游戏外挂和电影播放器传播，其主要攻击目标是游戏玩家和在线看视频的网民。中毒后的主要表现是主页被锁定为www.my2345.cc，杀毒软件反复报毒。

新鬼影病毒先判定当前系统主板BIOS是否为Award BIOS，然后再查找SMI端口，写入新的BIOS内容，其目的是保护硬盘MBR（主引导记录）不被其他程序改写。

5. Windows远程桌面蠕虫Morto

Morto蠕虫病毒会远程扫描开启了3389端口（远程服务通信端口）的电脑，猜解管理员口令，如果远程电脑碰巧使用了简单易被猜解的口令，就会导致电脑被黑客远程控制，此时电脑基本上就任由黑客摆布了。

扫描是入侵的前奏，用以发现可以入侵的弱点。金山防黑墙，用以检测和拦截黑客远程攻击。这些攻击已能被金山防黑墙成功防御。





3.3.3 升级杀毒软件病毒库

用户在使用杀毒软件时需经常为其病毒库进行升级，因为病毒在不断更新，杀毒软件的开发者也会不断地对病毒库更新，以便能查杀最新的电脑病毒。如果杀毒软件没有设置成自动升级，则需手动对其进行升级。



下面将以360杀毒软件为例，讲解升级杀毒软件的方法，其具体操作如下。



第1步：检查更新

启动360杀毒软件，选择“产品升级”选项卡，在其中单击 检查更新 按钮系统将进行病毒库升级，并显示升级进度。

提示：如要将360杀毒软件设置为自动升级，可单击“修改”超链接，在打开的对话框中选中“自动升级病毒特征库及数据”单选按钮，然后单击 确定 按钮即可。



第2步：完成升级

升级成功后，系统将提示升级完成，单击 确定 按钮返回升级界面，在其中将显示升级的日期、版本以及可拦截的挂马和钓鱼网址数。



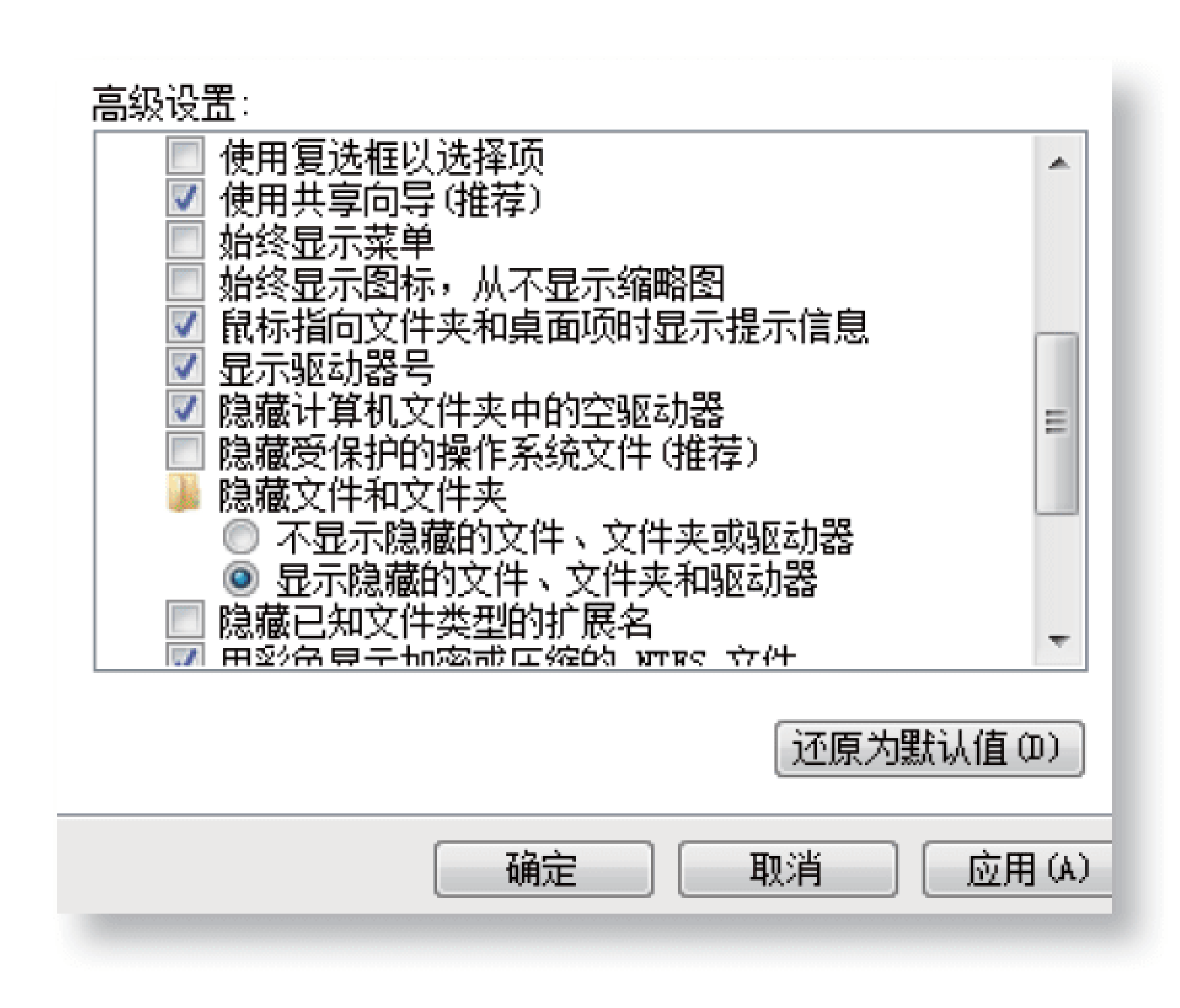
升级杀毒软件后对可疑程序进行扫描

首先对360杀毒软件进行升级，然后再对电脑进行全盘扫描，如电脑存在病毒，通过上网查询对其进行分析，如不能在网上查找到此病毒，则可将此病毒类型提交到360安全中心对其进行分析。

3.4　更进一步——轻松处理病毒和木马

通过阿伟的讲解，娜娜已经学会了使用杀毒软件查杀病毒，并且了解了该怎样对一些杀毒软件无法检测的病毒进行处理。虽然已经掌握了这些方法，但娜娜仍然想了解更多一些关于病毒和木马的知识，于是她又找到了阿伟。

第1招　手动清除电脑病毒



如果用户能轻易地辨别出电脑中的病毒文件，则可用手动清除的方法删除电脑病毒，使用这种方法首先应显示隐藏的文件。

①在“计算机”窗口中选择“组织”/“文件夹和搜索选项”命令。

②在打开的“文件夹选项”对话框中选择“查看”选项卡，在其下的列表框中选中“显示所有文件和文件夹”单选按钮，取消选中“隐藏受保护的操作系统文件”复选框。

③单击 确定 按钮应用设置，在磁盘中找到相应文件进行删除即可。



教你一招

创建与病毒同名文件

在Windows操作系统中，同一目录中同名的文件和文件夹是不能共存的，因此，为了防止感染病毒，用户可在硬盘各分区与U盘的根目录下手动创建一个与病毒文件autorun.inf名称相同的文件，使病毒无法在硬盘与U盘中自动生成病毒文件。除此之外，用户还应关闭系统的自动播放功能。

第2招 使用QQ医生清除盗号木马

QQ医生能有效清除盗号木马，其主界面非常简洁，打破了传统杀毒软件复杂的操作习惯，初学者能轻易上手。使用QQ医生清除盗号木马的方法如下：

①双击QQ医生快捷图标，打开其主界面，选择“扫描木马”选项卡。

②单击 开始扫描 按钮进行扫描，扫描完成后，在该窗口中自动显示扫描结果。

③若检测到威胁QQ的木马或病毒，系统将默认选中，执行清除操作即可。

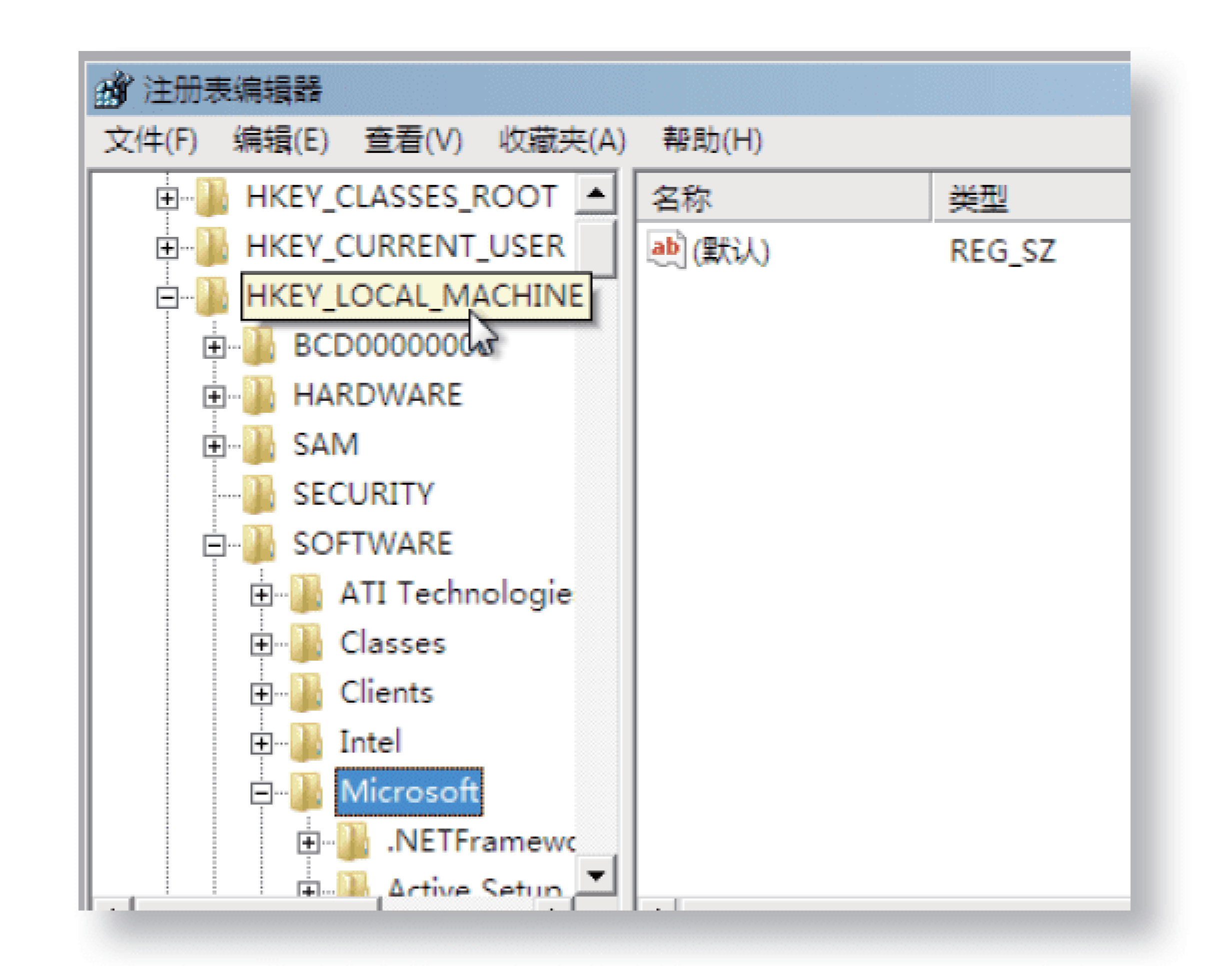


第3招 在安全模式下清除木马

在安全模式下对病毒和木马的清除是最彻底的，如已知木马的名称和对应的注册表项，则可在注册表中删除即可，其方法如下：

①启动电脑，按F8键，系统将显示模式列表，选择“安全模式”选项，按Enter键进入安全模式。

②打开“运行”对话框，在其中的文本框中输入“regedit”，按Enter键打开注册表，在其中进行相关操作即可。





冰河和灰鸽子木马文件

冰河木马的程序路径为“C:\WINDOWS\system32\Kernel32.exe”与“C:\WINDOWS\system32\Kernel32.dll”，灰鸽子木马的文件为“Game_hook.dll,Gamekey.dll,Game.dl”，在注册表中找到相应注册表项删除即可。

第4招 设置注册表权限防御病毒和木马

大部分的木马及部分的病毒是通过注册表的自启动项等实现自启动的。设置注册表自启动项为everyone只读（Run、RunOnce、RunService），可防止木马、病毒通过自启动项目启动。

如果在域环境里，可以通过活动目录的组策略实现；本地电脑也可进行组策略设置（命令行用secedit）。



第5招 清除端口木马

在互联网上，很多木马程序都是通过某个端口服务来攻击。下面就为大家介绍一些常见的木马程序攻击的端口及如何清除这些程序。

①使用netstat -an命令确定系统上是否开放了113端口。用fport命令查看监听113端口的程序。

②确定木马程序名后，在任务管理器中结束该进程。

③运行注册表管理程序，在注册表里查找该程序，并将相关的键值全部删掉。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -an

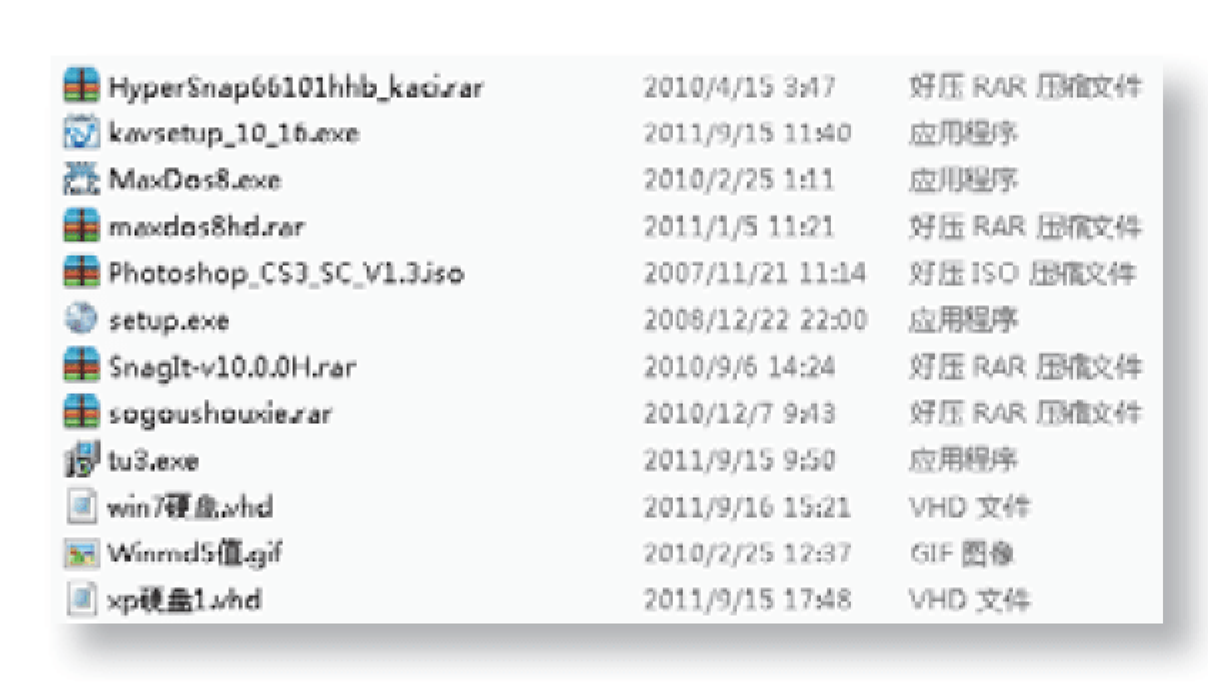
活动连接

  协议  本地地址              外部地址        状态
  TCP    0.0.0.0:80             0.0.0.0:0
  TCP    0.0.0.0:135            0.0.0.0:0
  TCP    0.0.0.0:445            0.0.0.0:0
  TCP    0.0.0.0:554            0.0.0.0:0
  TCP    0.0.0.0:2425           0.0.0.0:0
  TCP    0.0.0.0:2869           0.0.0.0:0
  TCP    0.0.0.0:10243          0.0.0.0:0
  TCP    0.0.0.0:49152          0.0.0.0:0
  TCP    0.0.0.0:49153          0.0.0.0:0
  TCP    0.0.0.0:49154          0.0.0.0:0
  TCP    0.0.0.0:49156          0.0.0.0:0
  TCP    0.0.0.0:49157          0.0.0.0:0
  TCP    0.0.0.0:63317          0.0.0.0:0
  TCP    192.168.1.20:139       0.0.0.0:0
```



3.5 活 学 活 用

（1）设置始终显示电脑中文件的扩展名，并在电脑中开启360木马防火墙。





（2）使用360杀毒软件对电脑进行全盘扫描，并开启实时防护，检测电脑中是否存在病毒或可疑程序。





高级启动选项

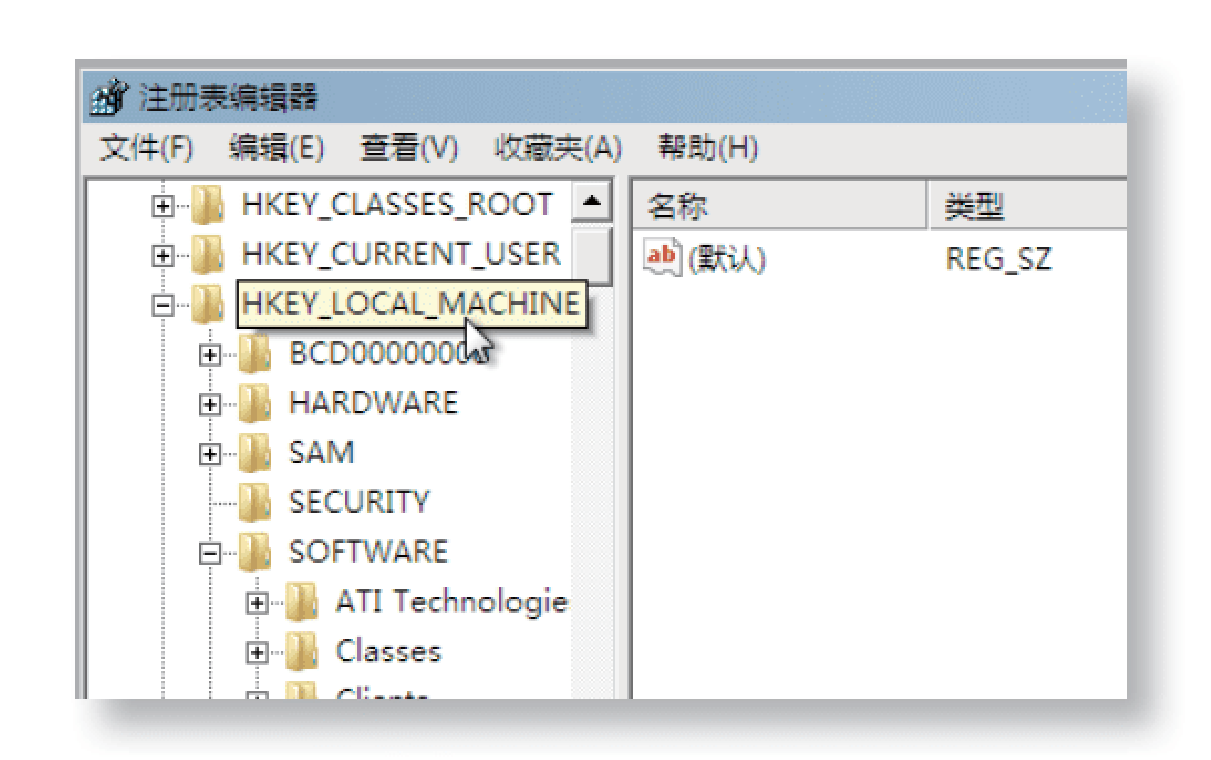
选择以下内容的高级选项：Windows 7
（使用箭头键以突出显示您的选择。）

修复计算机

安全模式
网络安全模式
带命令提示符的安全模式

启用启动日志
启用低分辨率视频(640x480)
最近一次的正确配置(高级)
目录服务还原模式
调试模式
禁用系统失败时自动重新启动
禁用驱动程序签名强制

（3）在安全模式下扫描病毒和木马，并在注册表中清除相关木马键值项。



（4）打开任务管理器，并在其中查看是否存在木马和病毒，如发现，则结束相关木马程序的进程。

映像名称	用户名	CPU	内存(...	描述
RtHDVCpl.exe	Admin...	00	228 K	Realtek...
SearchInde...	SYSTEM	00	8,936 K	Microso...
services.exe	SYSTEM	00	2,040 K	服务和...
smss.exe	SYSTEM	00	72 K	Windows...
Snagit32.exe	Admin...	04	8,916 K	Snagit
SnagitEdit...	Admin...	00	4,300 K	Snagit ...
SnagPriv.exe	Admin...	00	712 K	Snagit ...
spoolsv.exe	SYSTEM	00	684 K	后台处...
svchost.exe	SYSTEM	00	1,468 K	Windows...
svchost.exe	NETWO...	00	1,808 K	Windows...
svchost.exe	LOCAL...	00	4,136 K	Windows...
svchost.exe	SYSTEM	00	58,204 K	Windows...
svchost.exe	SYSTEM	00	4,904 K	Windows...
svchost.exe	LOCAL...	00	2,036 K	Windows...

提示：需了解系统的基本进程及其作用，并且查看系统中开启了哪些附加进程，以判断电脑中是否有木马程序正在运行。

（5）上网查找相关杀毒软件推出的新功能以及目前网络用户使用杀毒软件的情况，并对自己电脑中安装的杀毒软件进行升级。



（6）简述电脑病毒的特征，并对如何预防和清除电脑中出现的新病毒的方法进行总结说明。



☑ 还在担心他人使用自己的电脑吗？

☑ 想知道怎样保护电脑的安全吗？

☑ 还在为别人窥探电脑中的隐私而烦恼吗？

☑ 想知道怎样阻止别人登录自己的电脑吗？



第 04 章 限制他人使用电脑

娜娜今天很气愤，因为她电脑中的照片被别人到处散发，而且电脑中的很多重要数据也没有了。她想不让别人使用自己的电脑，但是却不知道怎样来设置。阿伟看见她烦恼的样子，了解情况后，就对她说："娜娜，看你急成这样子，怎么不早一点来问我呢？我可以教你怎样设置你的电脑，不让别人随便使用啊！"娜娜懊悔地说："是啊，不过你现在也可以教我啊！"

4.1　你的账户安全吗

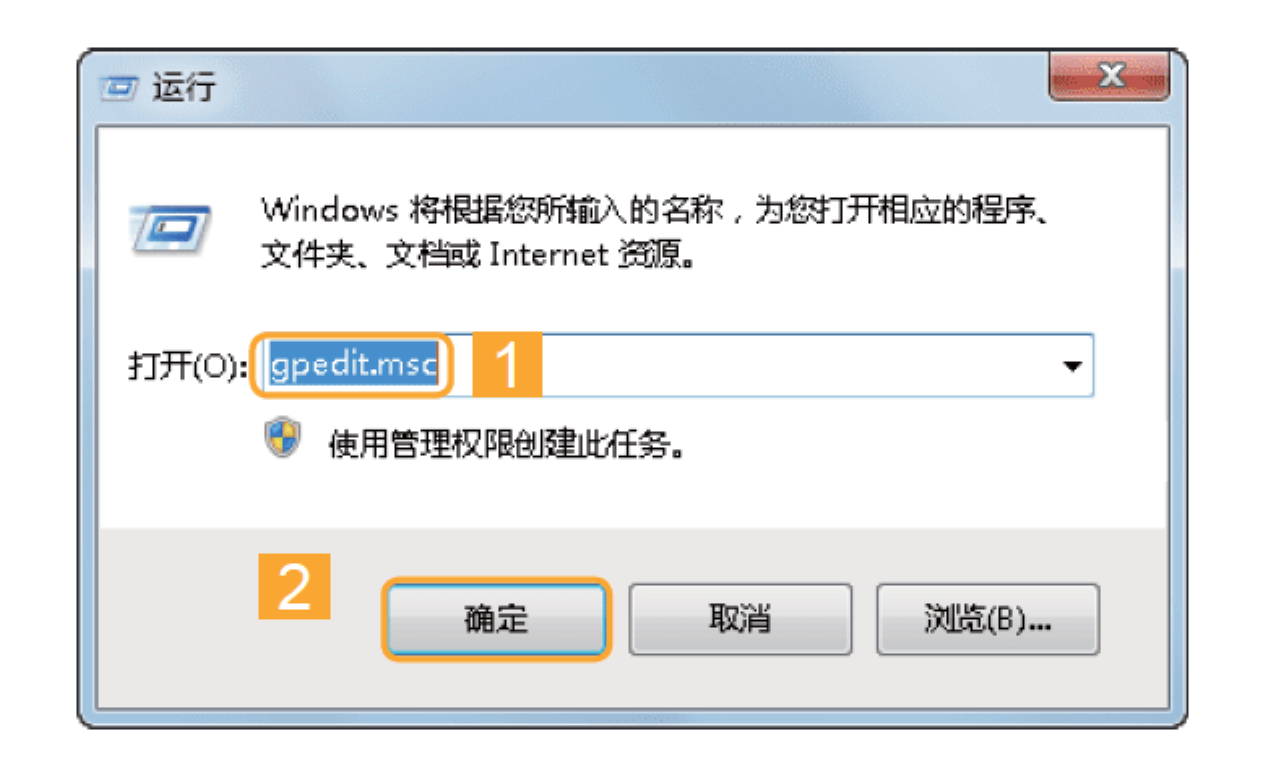
阿伟告诉娜娜：“要防止他人使用自己的电脑，首先应保障电脑账户的安全性。设置具有迷惑性的账户，让他人难以辨别系统管理员账户；禁用电脑中的来宾账户也可以很好地保障自己电脑不让他人随意访问……”还没等阿伟介绍完，娜娜便迫不及待地要求阿伟开始为她讲解。

4.1.1　重命名Administrator账户

Administrator账户是操作系统的超级用户管理员，它拥有操作系统的所有权限，如果被他人恶意利用，将是很危险的一件事情，也许你的隐私将不再保密，你的电脑也不再安全。因此，将其重命名能迷惑他人，使其不能轻易找到该账户。



下面将Administrator账户重命名为Star，其具体操作如下。

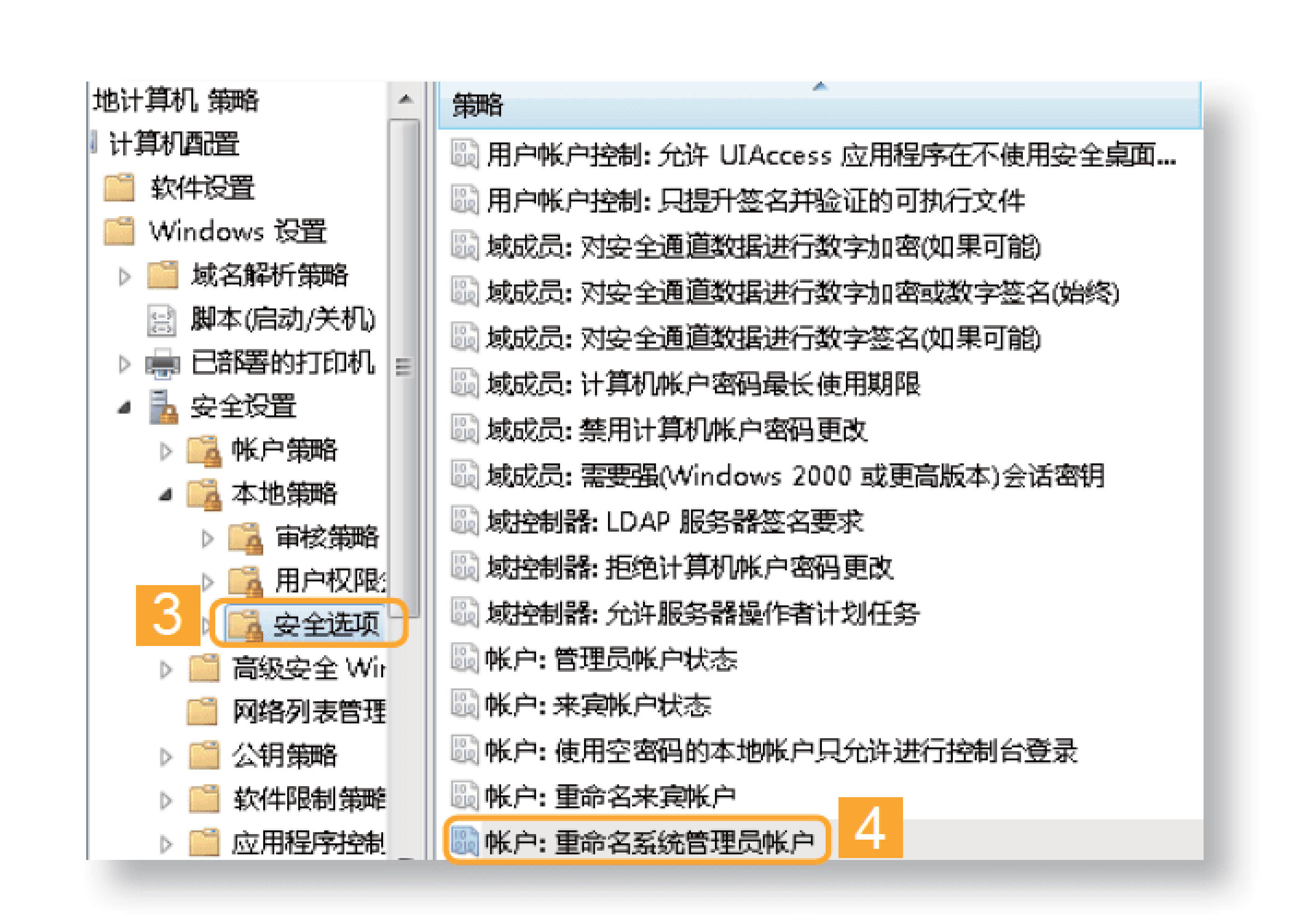


第1步：打开本地组策略编辑器

选择“开始”/“运行”命令，打开“运行”对话框，在其文本框中输入“gpedit.msc”，单击确定按钮，打开本地组策略编辑器。

第2步：展开安全选项

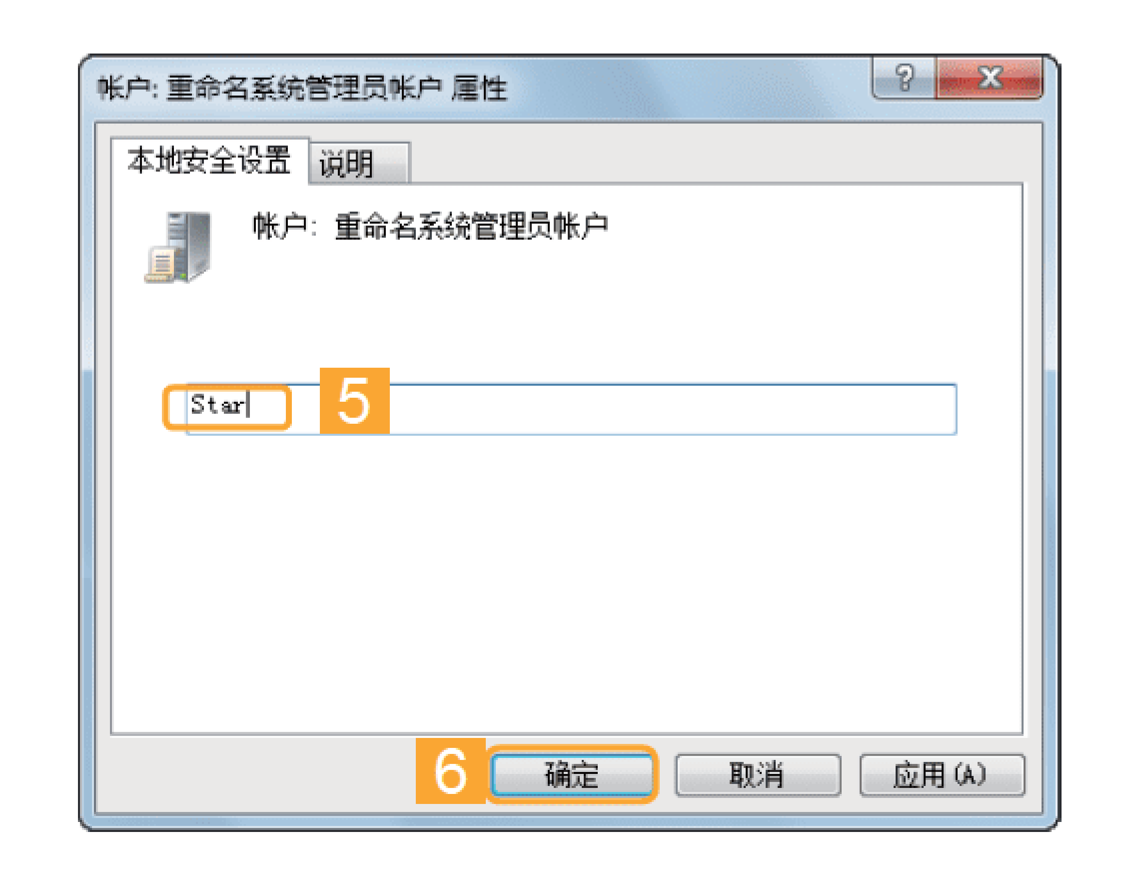
在打开窗口的左侧窗格中依次展开“计算机配置/Windows设置/安全设置/本地策略/安全选项”选项，然后在右侧窗格中双击“账户:重命名系统管理员账户”选项。





第3步：重命名账户名

在打开对话框的账户名称文本框中将Administrator修改为Star，然后单击 确定 按钮确认修改，重新启动电脑即可。



提示：此安全设置有利于提高Administrator账户的安全性，使超级用户的权限不易被窃取，因为重命名Administrator账户会使未授权的人猜测此权限用户名和密码组合的难度增加。

4.1.2 禁用来宾账户

很多网络中的非法入侵系统等操作都是通过系统的来宾账户（Guest）进行的，从而使电脑处于被他人控制的状态。针对这个问题，可以采用禁用来宾账户的方法防止他人访问的目的。



下面将以在控制面板中禁用来宾账户为例进行讲解，其具体操作如下。

第1步：打开用户账户窗口

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“添加或删除用户账户”超链接。



第2步：禁用来宾账户

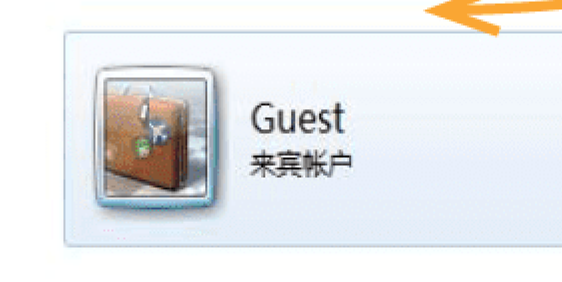
在打开的“选择希望更改的账户”窗口中单击“来宾账户”图标，打开“您想更改来宾账户的什么？”窗口，单击“关闭来宾账户”超链接即可完成操作。



您想更改来宾帐户的什么?

更改图片

关闭来宾帐户 4



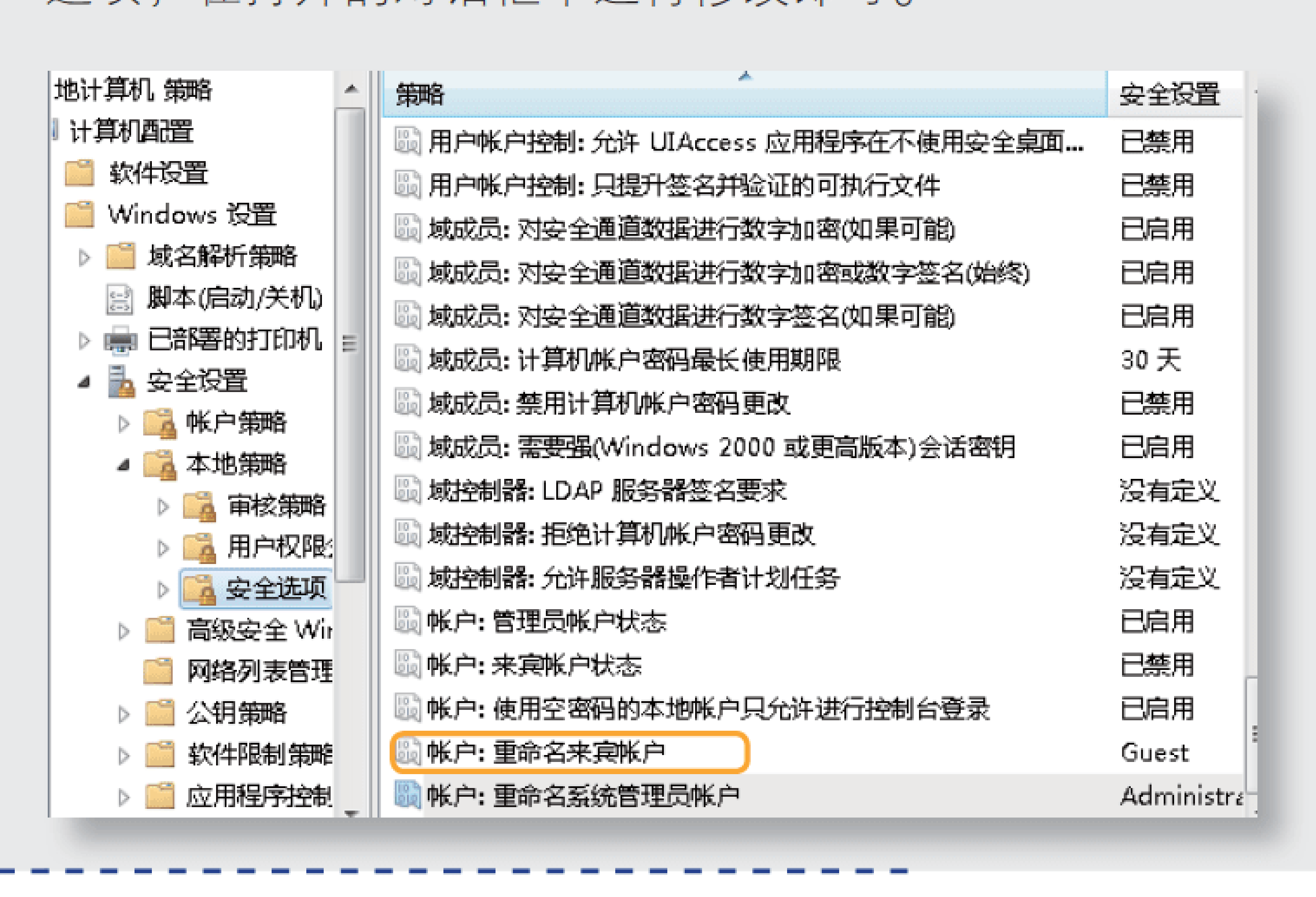
提示：要启用来宾账户，则只需单击“来宾账户”图标后，在打开的窗口中单击 启用 按钮。

教你一招

重命名来宾用户

禁用来宾账户后，带来的最直接的问题就是其他用户无法正常访问你的文件夹，也就是说无法实现“互连互通”。所以，我们可对来宾账户（Guest）重命名以解决此问题。

打开组策略编辑器，依次展开“计算机配置/Windows设置/安全设置/本地策略/安全选项”选项，然后在右侧窗口中找到并双击“账户:重命名来宾账户”选项，在打开的对话框中进行修改即可。



提示：来宾账户的权限很低，但对于黑客有很大的利用价值。一般情况下，如果没有监控软件，黑客利用来宾账户控制电脑，这些操作是看不到的。



4.1.3 创建另一个管理员账户

在操作系统中，用户可以创建一个管理员账户，使用不同的身份登录电脑，新创建的管理员账户将不会影响用户正常使用电脑，它仍然具备完全控制电脑的权限，同时用户可以为其设置密码，防止他人使用。



下面将以Administrator账户登录电脑创建一个名为Evan的管理员账户，并设置账户密码，其具体操作如下。

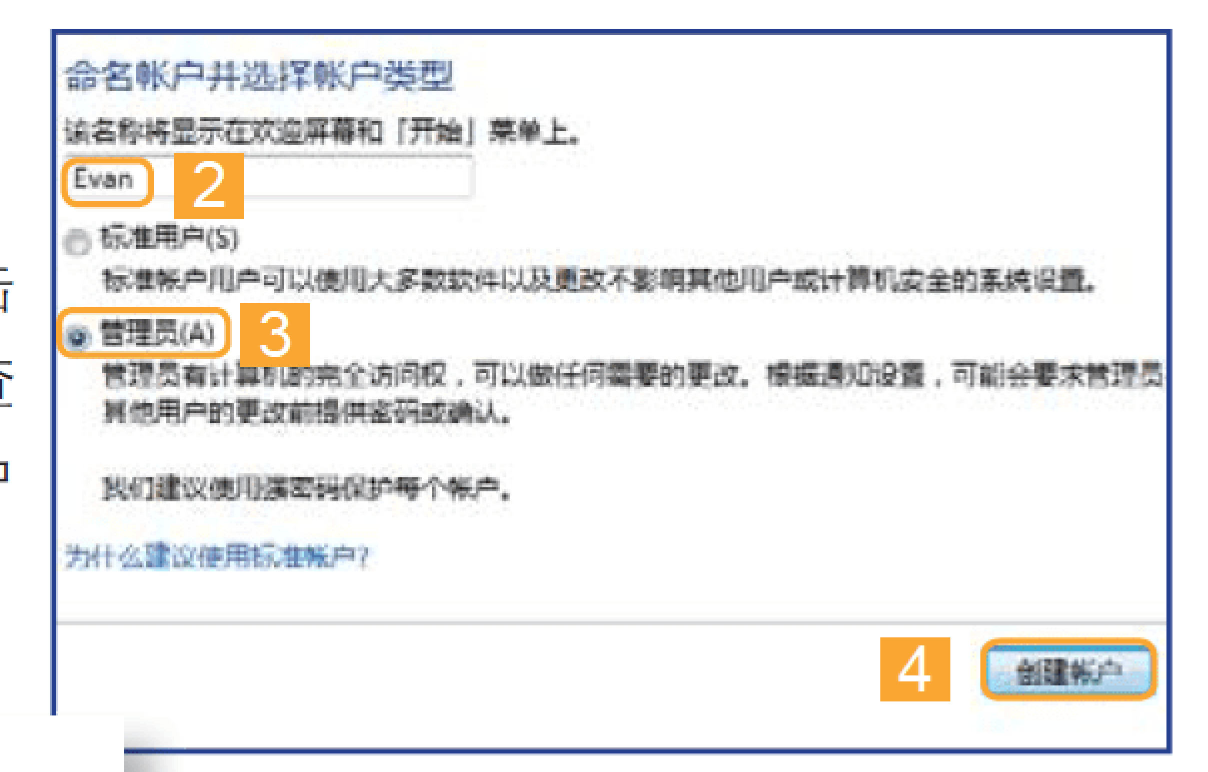


第1步：创建新账户

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“添加或删除用户账户”超链接，在打开的窗口中单击“创建一个新账户”超链接。

第2步：设置账户名和账户类型

在打开窗口的文本框中输入“Evan”，然后选中“管理员”单选按钮，单击创建帐户按钮，在返回的账户列表中可查看到新建的账户图标，然后单击该用户账户。

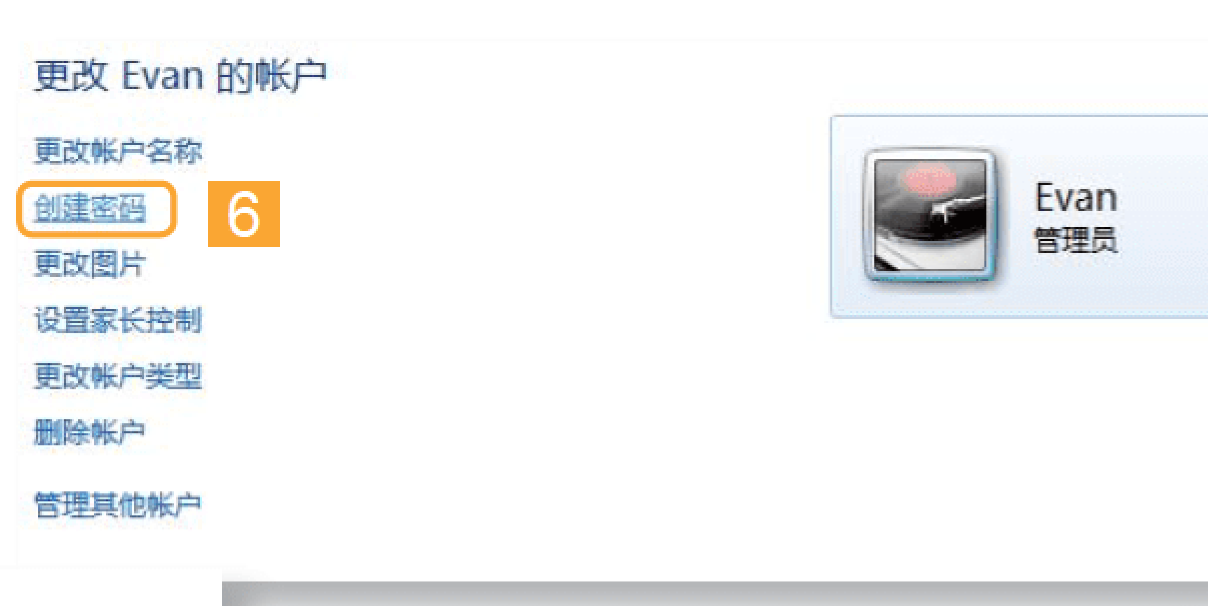




提示：用户在创建Evan管理员账户重启电脑后，其超级管理员账户Administrator将可能从启动的账户列表中消失。

第3步：**设置密码**

在打开的窗口中单击“创建密码”超链接，再在打开的窗口中设置账户的密码和密码提示，然后单击 创建密码 按钮完成密码的创建。



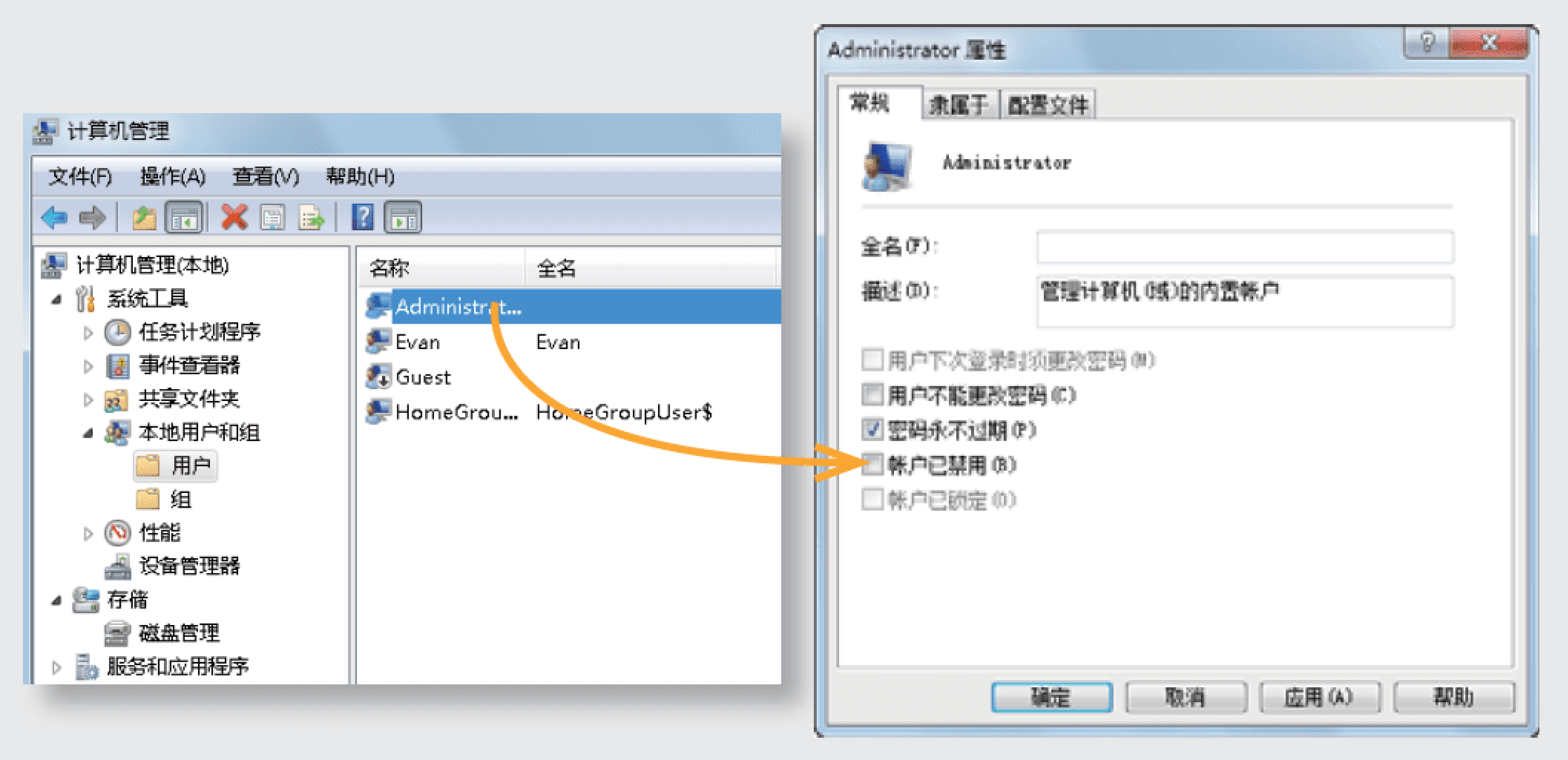


提示：在“更改Evan的账户”窗口中除创建密码外，还可以单击相应超链接对此账户进行更改账户名称、更改图片、设置家长控制、更改账户类型和删除账户等操作。

新手解惑

Q：怎样使消失的Administrator账户重新显示出来？

A：在桌面上右击“计算机”，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”对话框，然后展开左侧的“本地用户和组/用户”选项，在右侧双击Administrator用户项，在打开的对话框中取消选中“账户已禁用”复选框，最后单击 确定 按钮即可。





跟我练习

娜娜为了让自己的账户更安全，决定按照阿伟的讲解对自己的电脑进行相关设置

任务1：将自己电脑的管理员账户（Administrator）禁用，然后将来宾账户（Guest）重命名为Administralor。

任务2：创建一个管理员账户，将其命名为nana。

4.2 怎样安全登录电脑

阿伟发现娜娜的电脑仅仅设置简单的密码并且还不设防，于是对她说：“娜娜，难怪你的电脑经常被别人随意使用，这么简单的登录方式怎么行呢？我还是教教你怎样设置电脑的安全登录方式吧！”娜娜听了阿伟的话，心想：“还可以怎样来设置呢？”赶忙要求阿伟为她讲解。

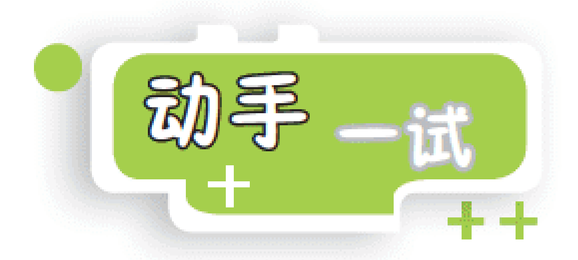
新手解惑

Q：通过哪些登录方式的设置能保证电脑的安全登录？

A：电脑的安全登录可通过设置BIOS登录密码、锁定无效的登录、不显示上一次登录信息以及离开时锁定电脑等方式来实现。

4.2.1 在BIOS中设置登录密码

在BIOS中设置电脑的登录密码可看作访问电脑的第一屏障，此密码包括开机密码和超级用户的密码，通过设置能有效阻止他人进入操作系统中读取重要信息。



下面将启动电脑，按Delete键进入BIOS界面，在其中设置登录系统的相关密码，其具体操作如下。



第1步：设置超级用户密码

在BIOS主界面选择Set Supervisor Password选项，在弹出的提示对话框中输入要设置的密码，然后按Enter键，确认输入。

教你一招

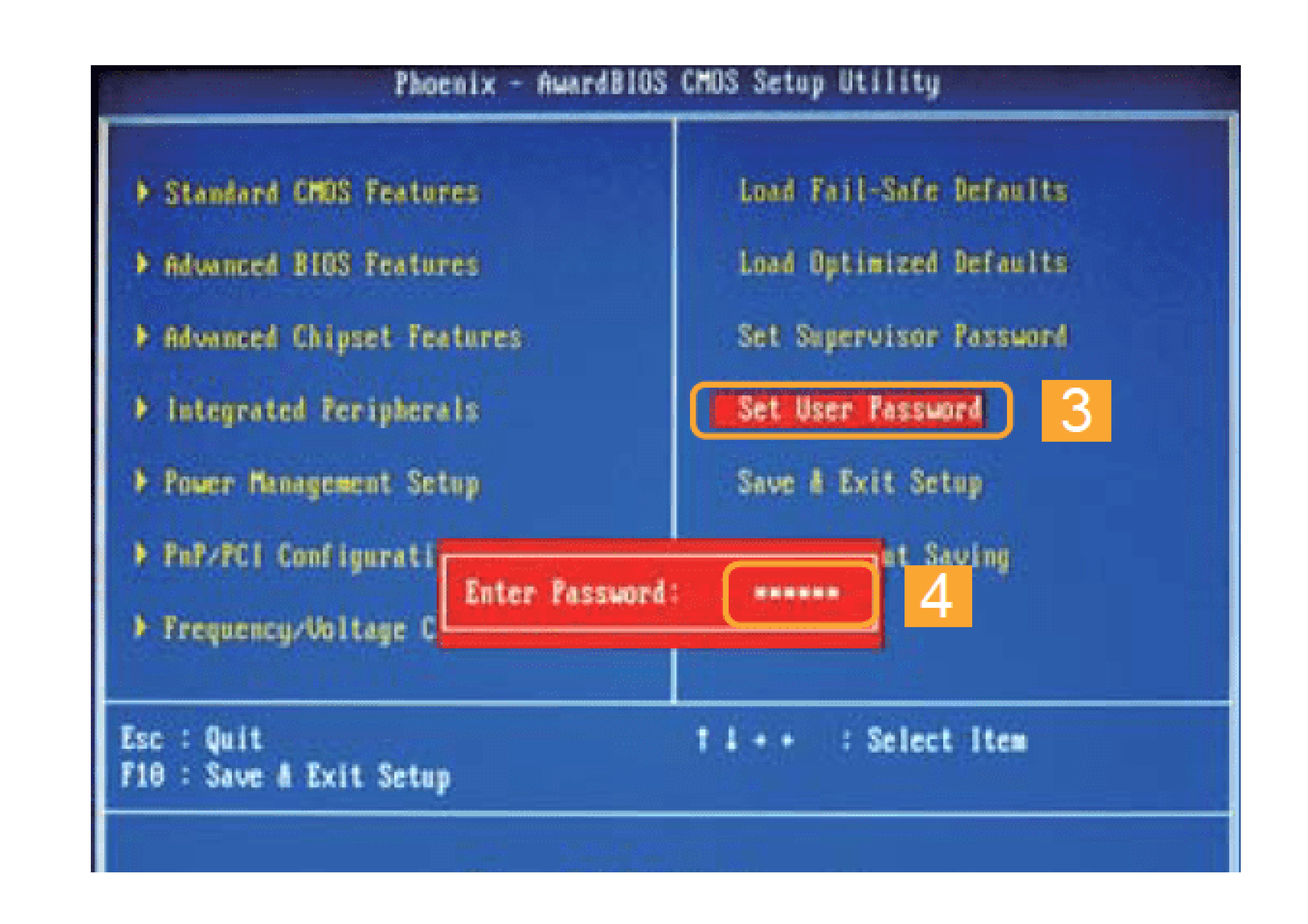
设置超级用户密码

该密码也可进入系统中进行设置，其对应的系统账户为Administrator。

第2步：设置开机密码

选择Set User Password选项，在弹出的提示对话框中输入密码，按Enter键确认输入。

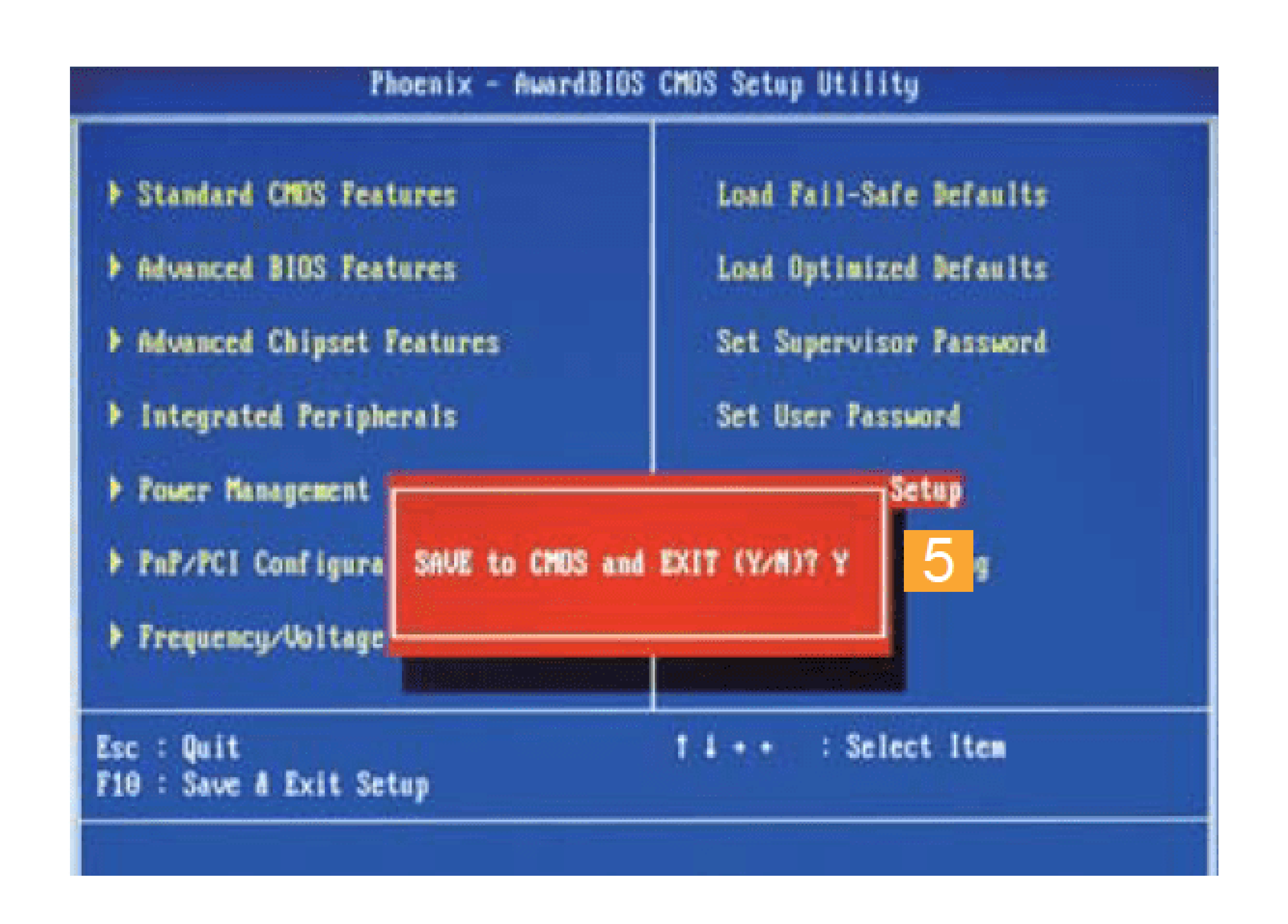
提示：开机密码应该与超级用户密码有所区别，这样才能起到双重保护的作用。





第3步：保存并退出BIOS

设置完成后，选择Save&Exit Setup选项，在弹出的提示对话框中输入“Y”，按Enter键，保存设置并退出BIOS设置界面。



提示：不同品牌的主板，其BIOS界面中设置项的位置会有所不同。



退出并保存设置

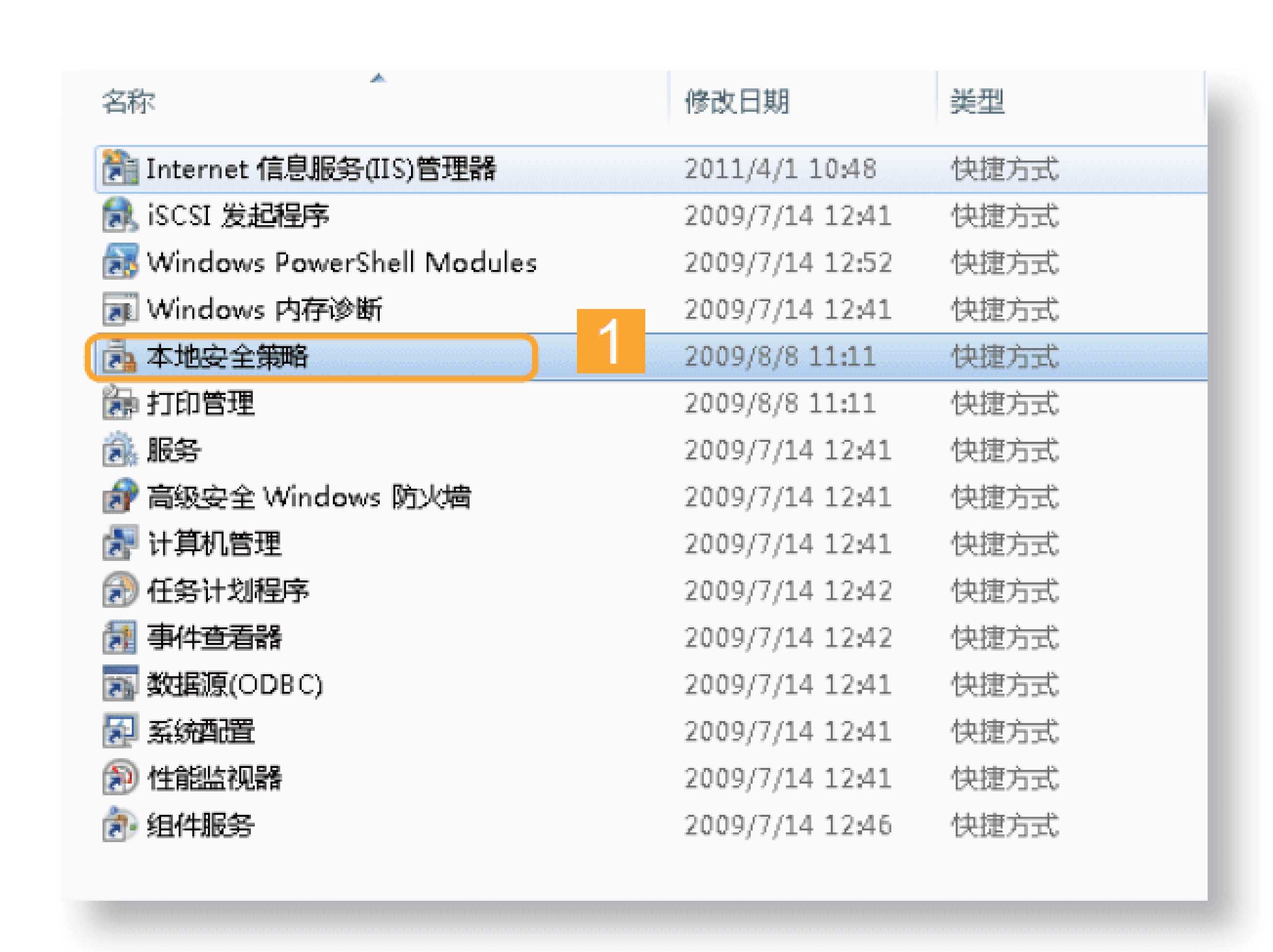
如要退出BIOS设置，也可按F10键进行保存并退出界面的操作。

4.2.2 锁定无效登录

为了防止他人进入电脑时反复用猜测密码的方式登录，可以锁定无效登录。当输入错误密码达到设置的次数时，系统将锁定此账户，并在一定时间内不能再次使用该账户。

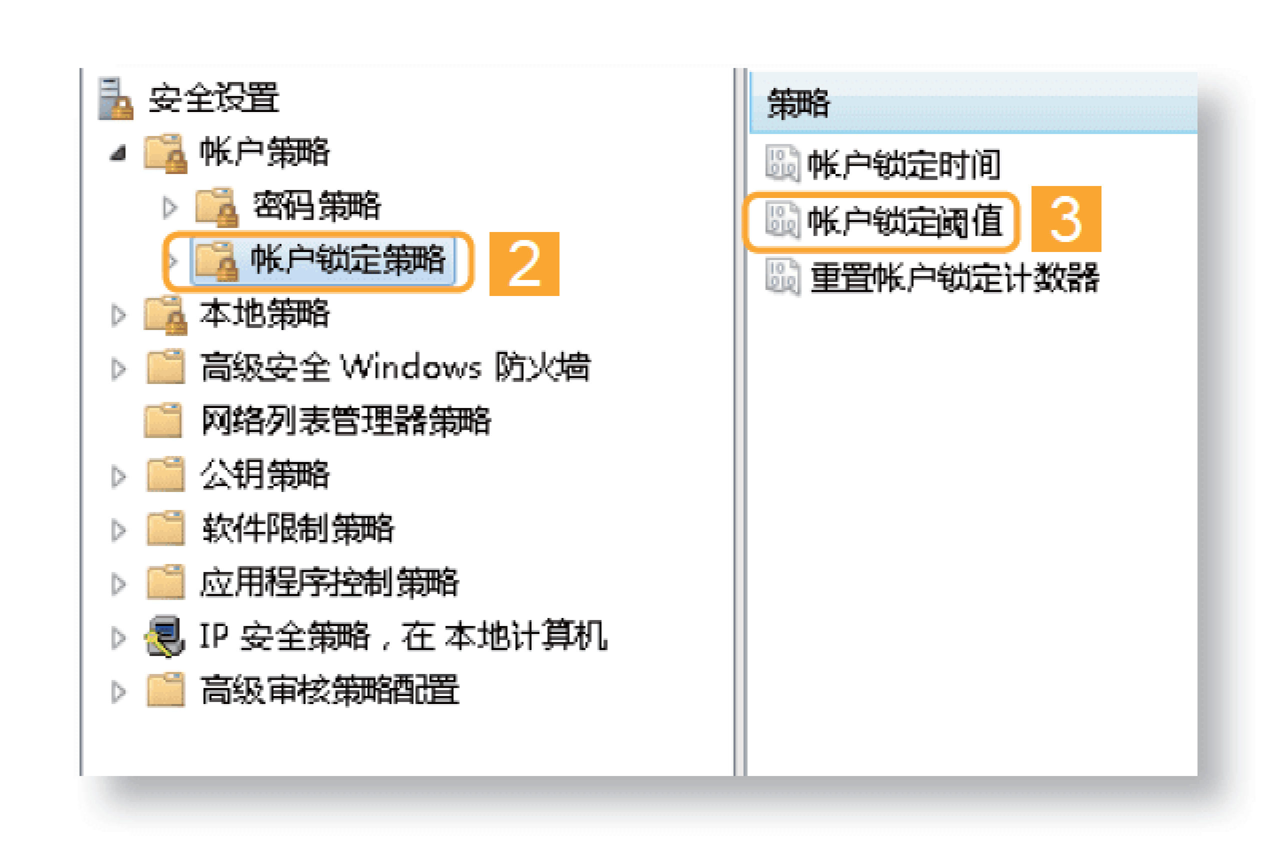


下面将以设置登录某个账户时，输入密码不超过3次，输入错误后锁定账户30分钟为例来讲解锁定无效登录的方法，其具体操作如下。



第1步：打开本地安全策略

选择“开始”/“控制面板”命令，打开“控制面板”窗口，然后单击“管理工具”超链接，在打开的“管理工具”窗口中双击“本地安全策略”选项，打开“本地安全策略”窗口。

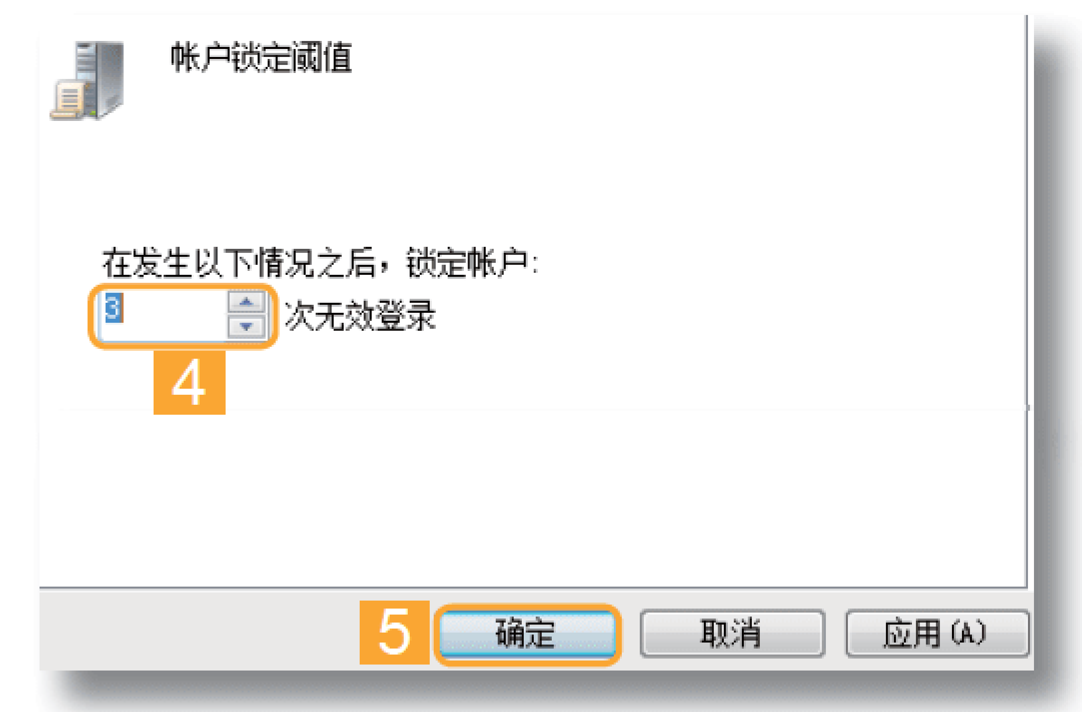


第2步：展开账户锁定策略

在打开窗口的左侧窗格中依次展开“安全设置/账户策略/账户锁定策略”选项，在右侧窗格中可以查看到“账户锁定时间”和“账户锁定阈值”设置项。

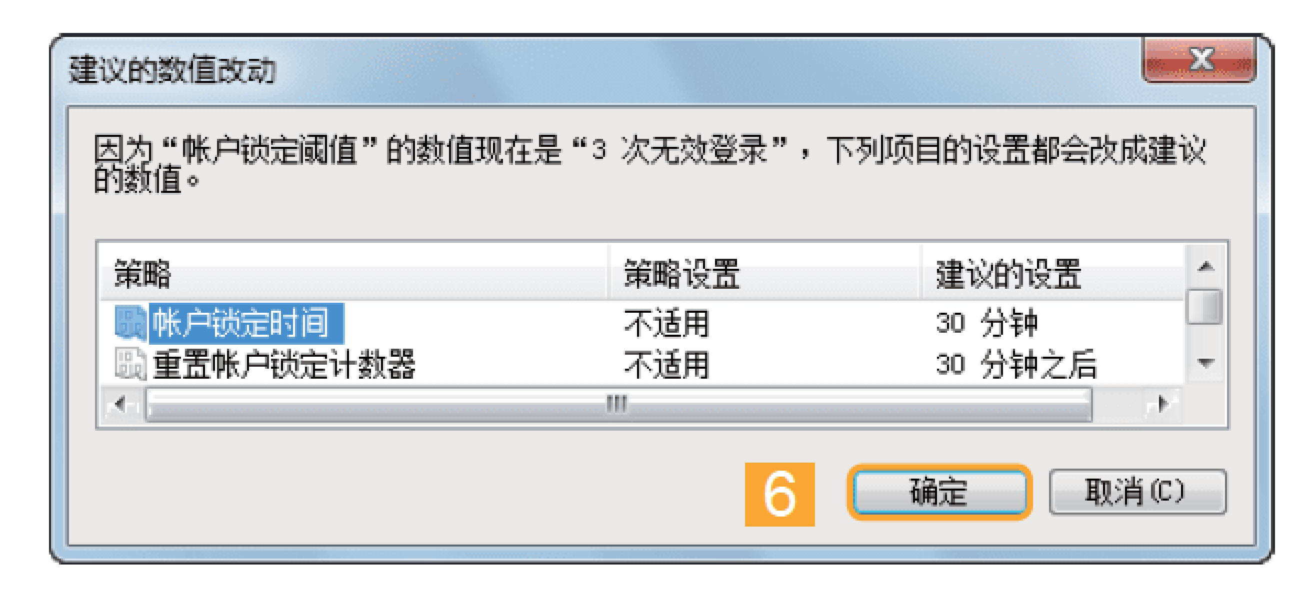
第3步：设置账户锁定阈值

双击“账户锁定阈值”选项，在打开对话框的数值框中输入“3”，然后单击 确定 按钮。



第4步：设置账户锁定时间

在打开的“建议的数值改动”提示对话框中将显示更改前的策略设置和建议的设置，这里保持默认设置，然后单击 确定 按钮即可将锁定时间设置为30分钟。



4.2.3 不显示上一次登录名

默认情况下，系统将保留上一次的登录用户名，这方便用户再次登录，却留下了安全隐患，不良企图者只需输入密码便可尝试登录，因此，用户可将上一次登录名隐藏以防止他人的访问。



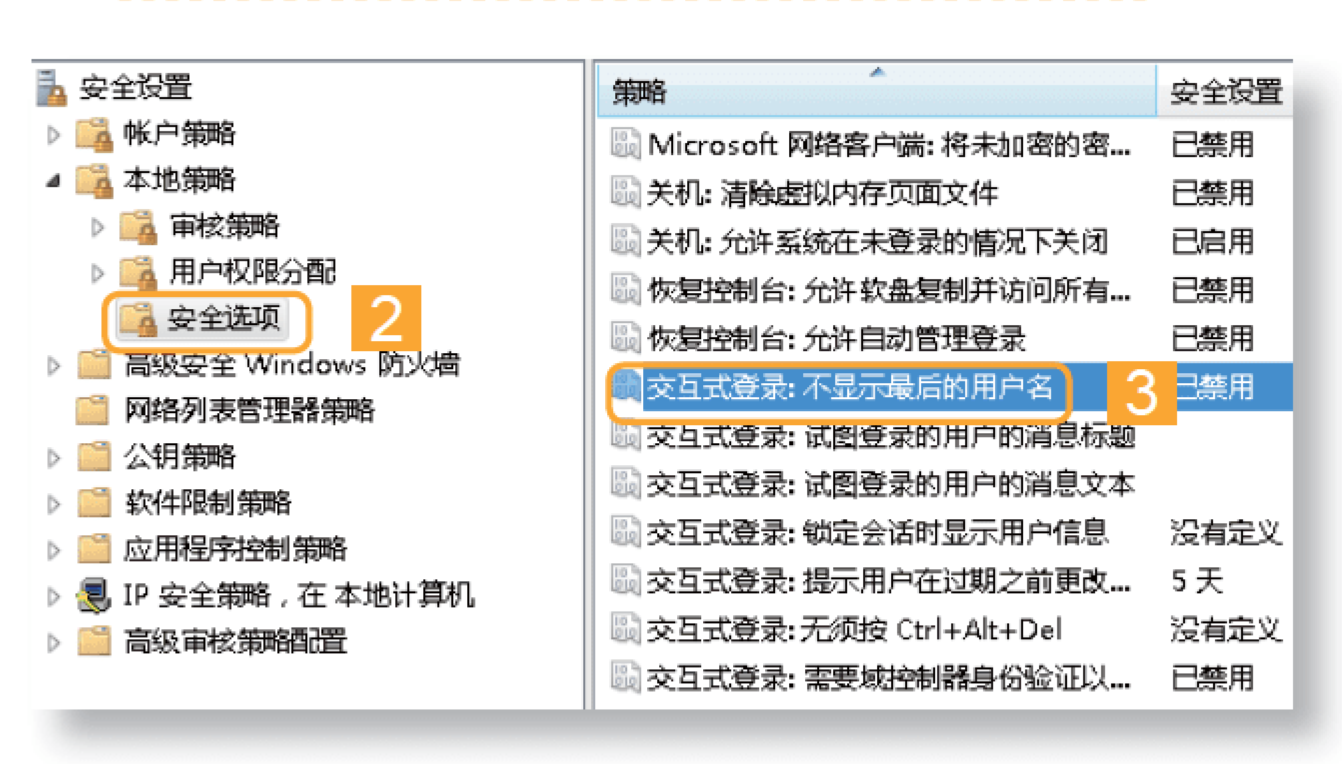
下面将在“本地安全策略”窗口中设置不显示上一次登录账号名，其具体操作如下。





第1步：展开安全选项

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“管理工具”超链接，在打开的窗口中双击“本地安全策略”选项打开该窗口。

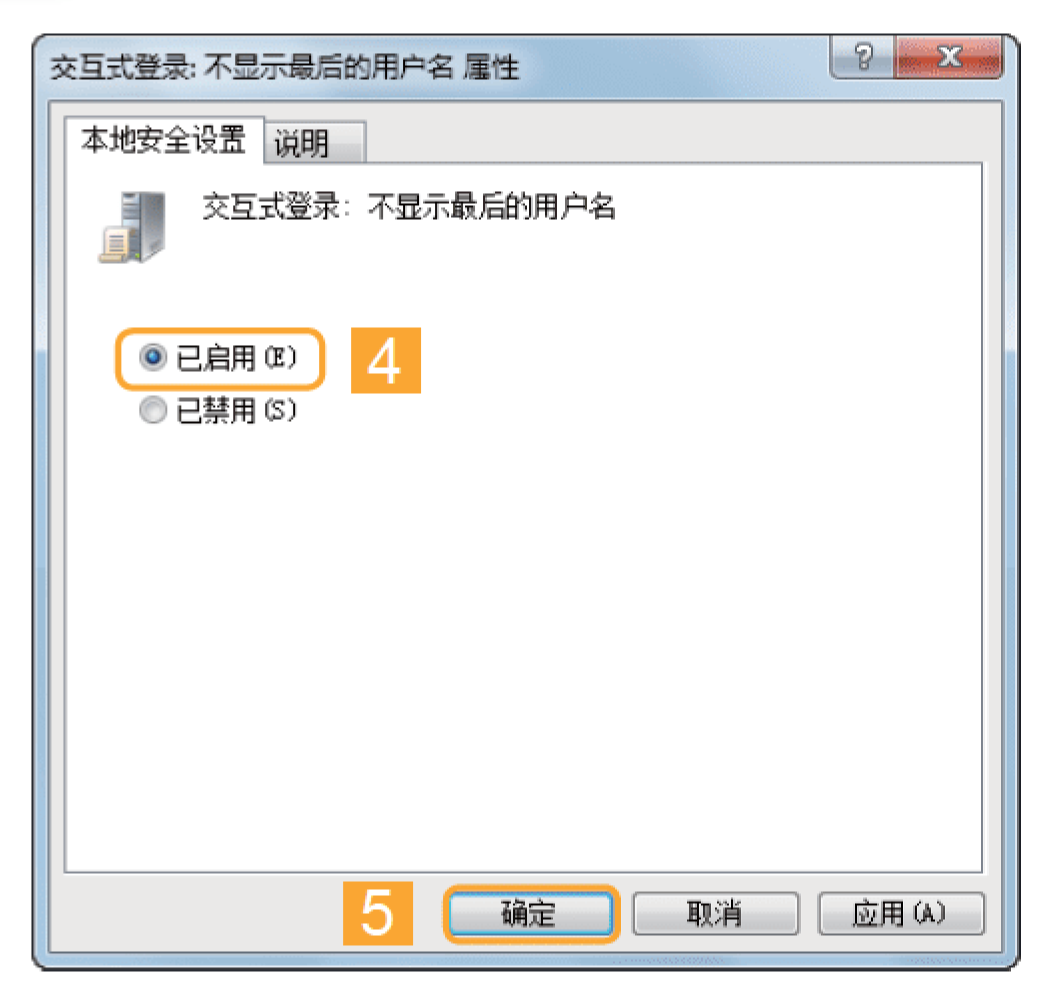


第2步：展开安全选项

在打开的“本地安全策略”窗口左侧窗格中展开“本地策略/安全选项”选项，然后双击右侧窗格中的“交互式登录：不显示最后的用户名”选项。

第3步：启用策略

在打开的对话框中选中“已启用”单选按钮，然后单击 确定 按钮。



提示：进行此设置后，系统启动或注销后，登录框中的用户名将为空，必须输入完整的用户名和密码才能登录电脑。

4.2.4 离开时锁定电脑

为了防止用户在离开自己的电脑后被其他人使用，可设置离开时锁定电脑的时间间隔，电脑自动锁定后，当需要使用时，需输入用户名和密码才能进入系统进行操作。



下面将设置离开电脑后5分钟自动锁定电脑，其具体操作如下。



第1步：打开“电源选项”窗口

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“电源选项”超链接，打开“电源选项”窗口。

第2步：更改计划设置

在打开的窗口中选中“节能”单选按钮，然后单击“更改计划设置”超链接。



第3步：设置锁定时间

在打开窗口的“关闭显示器”下拉列表框中选择“5分钟”选项，在“使计算机进入睡眠状态”下拉列表框中选择“5分钟”选项，然后单击 保存修改 按钮保存设置。





提示：设置成功后，当用户暂时不使用电脑时，系统将自动锁定账户，锁定后如要进入操作系统，则需输入用户名和密码才能重新进入。



提示：除了设置自动锁定电脑外，还可以按Windows+L键快速锁定电脑，这两种方法的效果相同。

跟我练习

在电脑中进行用户安全登录并完成设置后，可有效保障电脑不被他人随意使用

任务1：进入BIOS，设置超级用户密码和电脑的开机密码，完成后重启电脑，检验设置后的效果。

任务2：设置使用账户和密码登录系统，重新启动电脑后在登录账号的列表中不显示上一次登录名。

任务3：为了防止自己离开电脑时他人使用你的电脑，可以设置自动锁定电脑以解决此麻烦。



策略	安全设置
Microsoft 网络客户端：将未加密的密...	已禁用
关机：清除虚拟内存页面文件	已禁用
关机：允许系统在未登录的情况下关闭	已启用
恢复控制台：允许软盘复制并访问所有...	已禁用
恢复控制台：允许自动管理登录	已禁用
交互式登录：不显示最后的用户名	已禁用
交互式登录：试图登录的用户的消息标题	
交互式登录：试图登录的用户的消息文本	
交互式登录：锁定会话时显示用户信息	没有定义
交互式登录：提示用户在过期之前更改...	5 天
交互式登录：无须按 Ctrl+Alt+Del	没有定义
交互式登录：需要域控制器身份验证以...	已禁用

4.3 设置用户权限

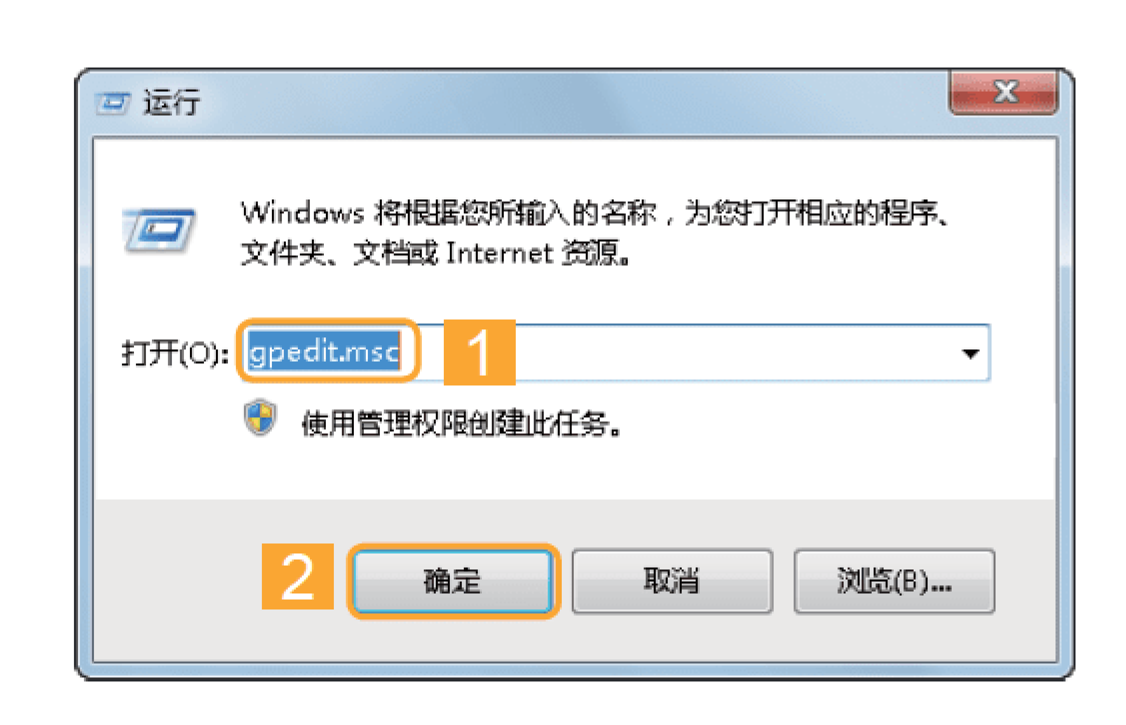
娜娜很郁闷，她电脑中的数据又不见了，由于公司的电脑是很多人共用的，因此她电脑中的数据经常被别人删除，她很早就让阿伟想想办法，但是阿伟一直都没空来给她解决这个问题，今天正好阿伟没什么事，于是娜娜就找到他，让他快想想办法。阿伟听了后告诉她，可以通过设置用户的使用权限来限制别人对数据的操作权限，从而解决这个问题。

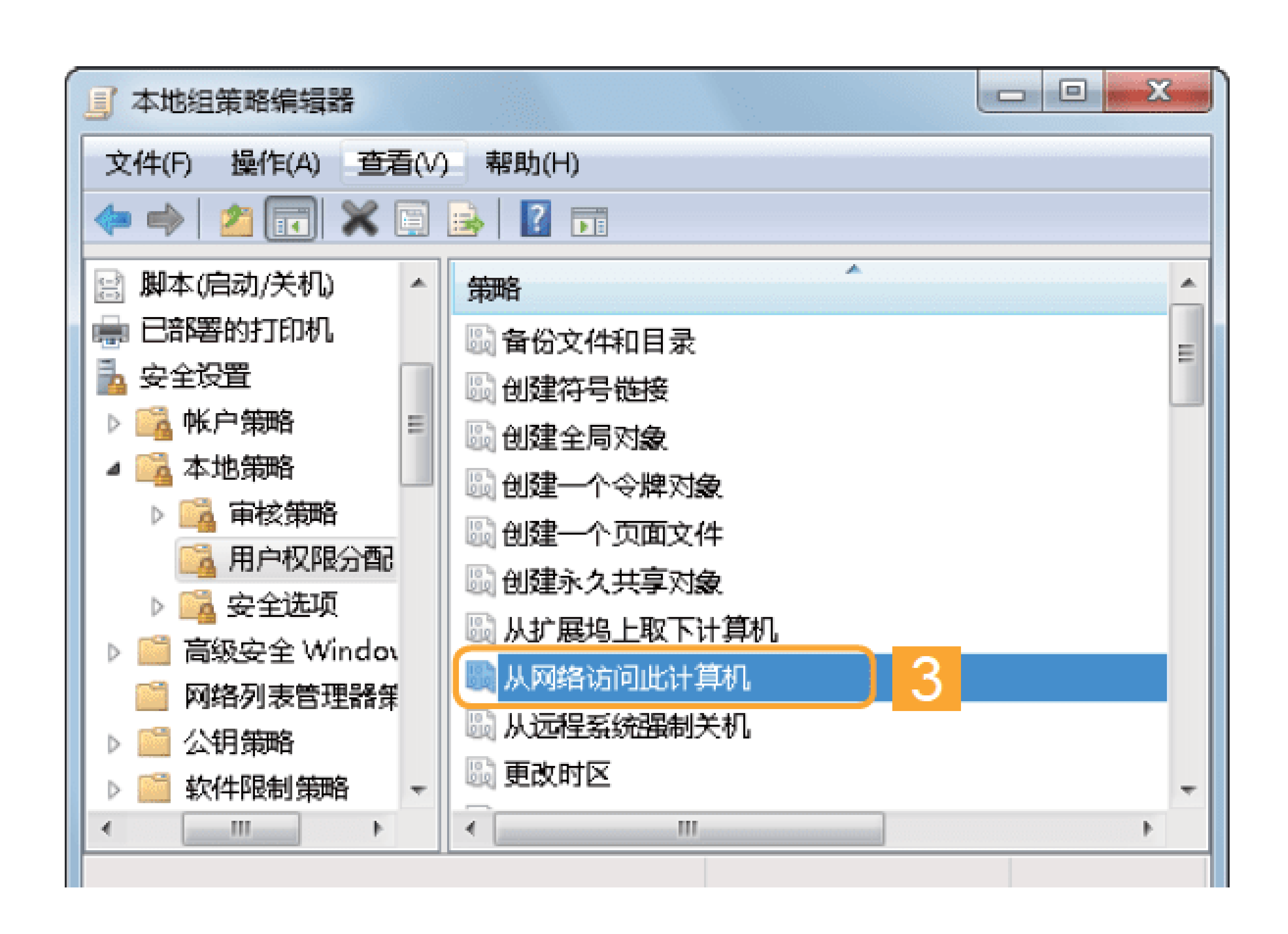


下面将在组策略中设置电脑只允许管理员和Evan账户访问，其他账户拒绝访问，达到限制他人对数据操作的目的，其具体操作如下。

第1步：打开本地组策略编辑器

在“运行”对话框的“打开”下拉列表框中输入“gpedit.msc”，然后单击 确定 按钮，打开本地组策略编辑器。



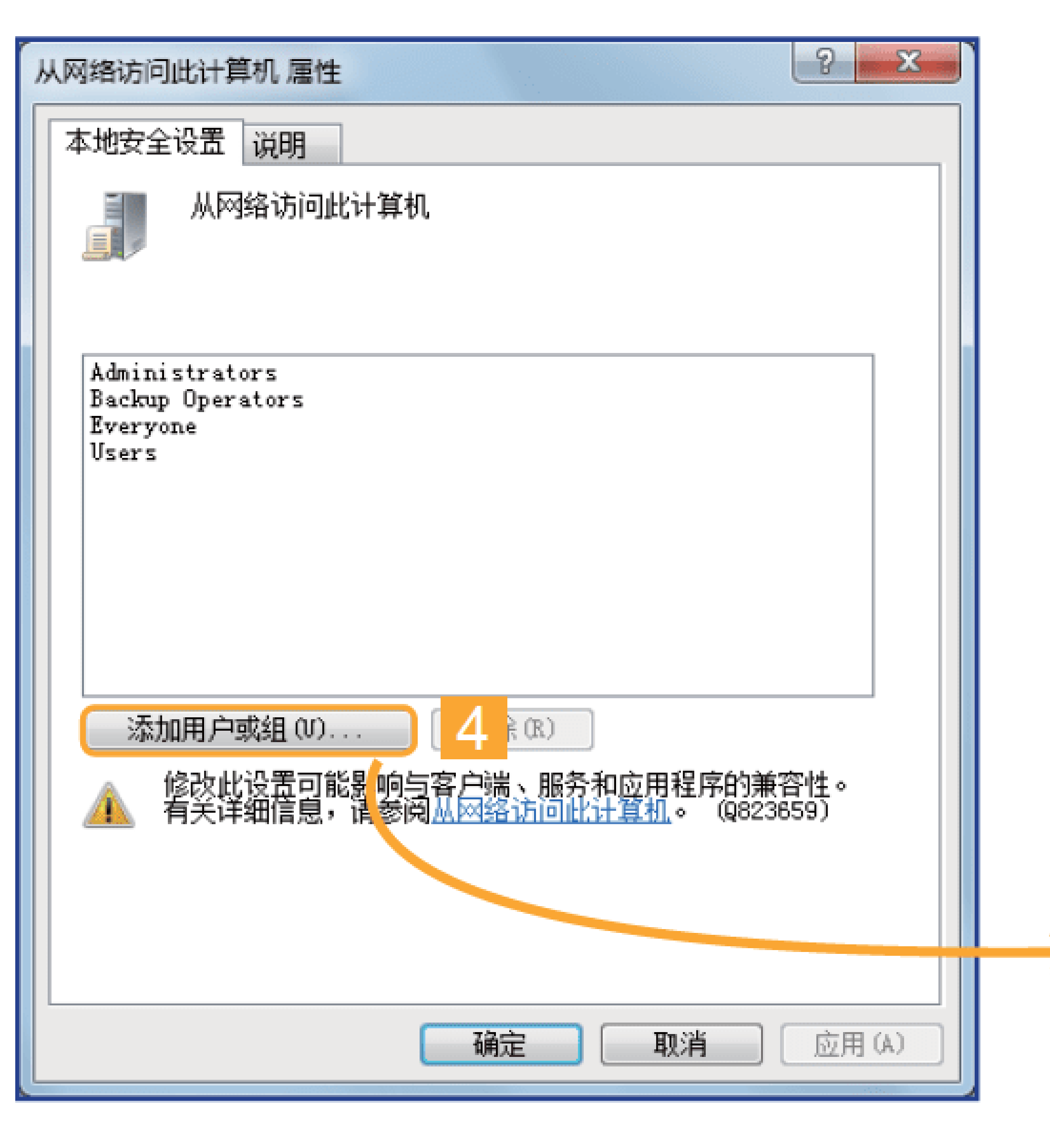


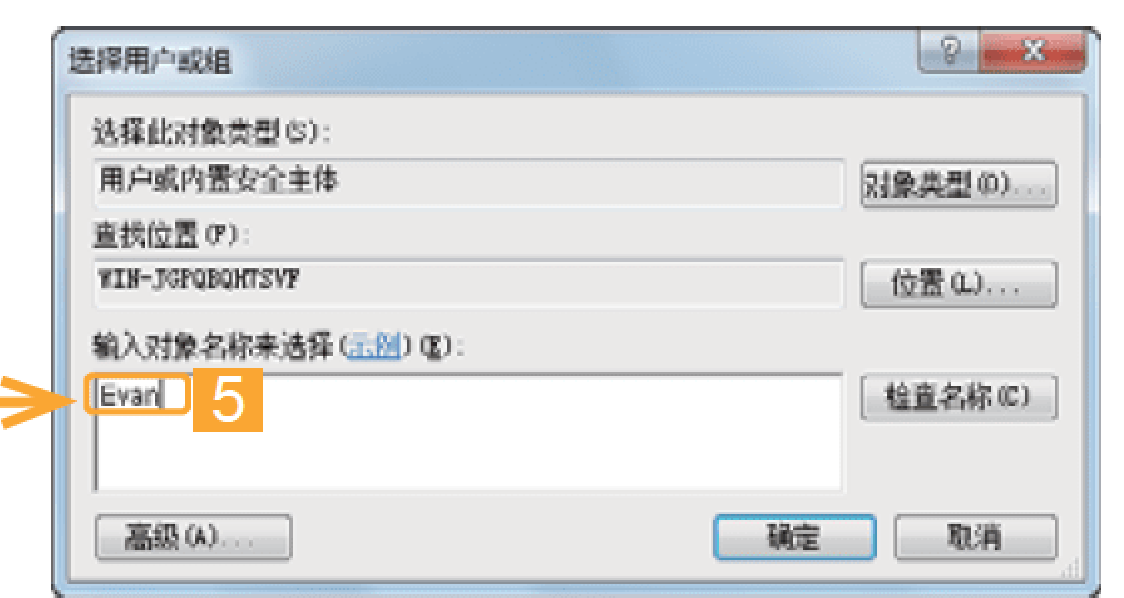
第2步：选择从网络访问此计算机

在打开窗口的左侧窗格中依次展开“计算机配置/Windows设置/安全设置/本地策略/用户权限分配”选项，在右侧窗格中双击需要改变的用户权限选项，这里双击“从网络访问此计算机”选项。

第3步：输入用户名称进行查找

在打开的“从网络中访问此计算机 属性”对话框中单击 添加用户或组(U)... 按钮，在打开对话框的“输入对象名称来选择”文本框中输入“Evan”。







第4步：检查用户是否存在

单击检查名称(C)按钮，如输入的用户存在，则在文本框中将显示电脑的名称和用户的名称，然后单击确定按钮。



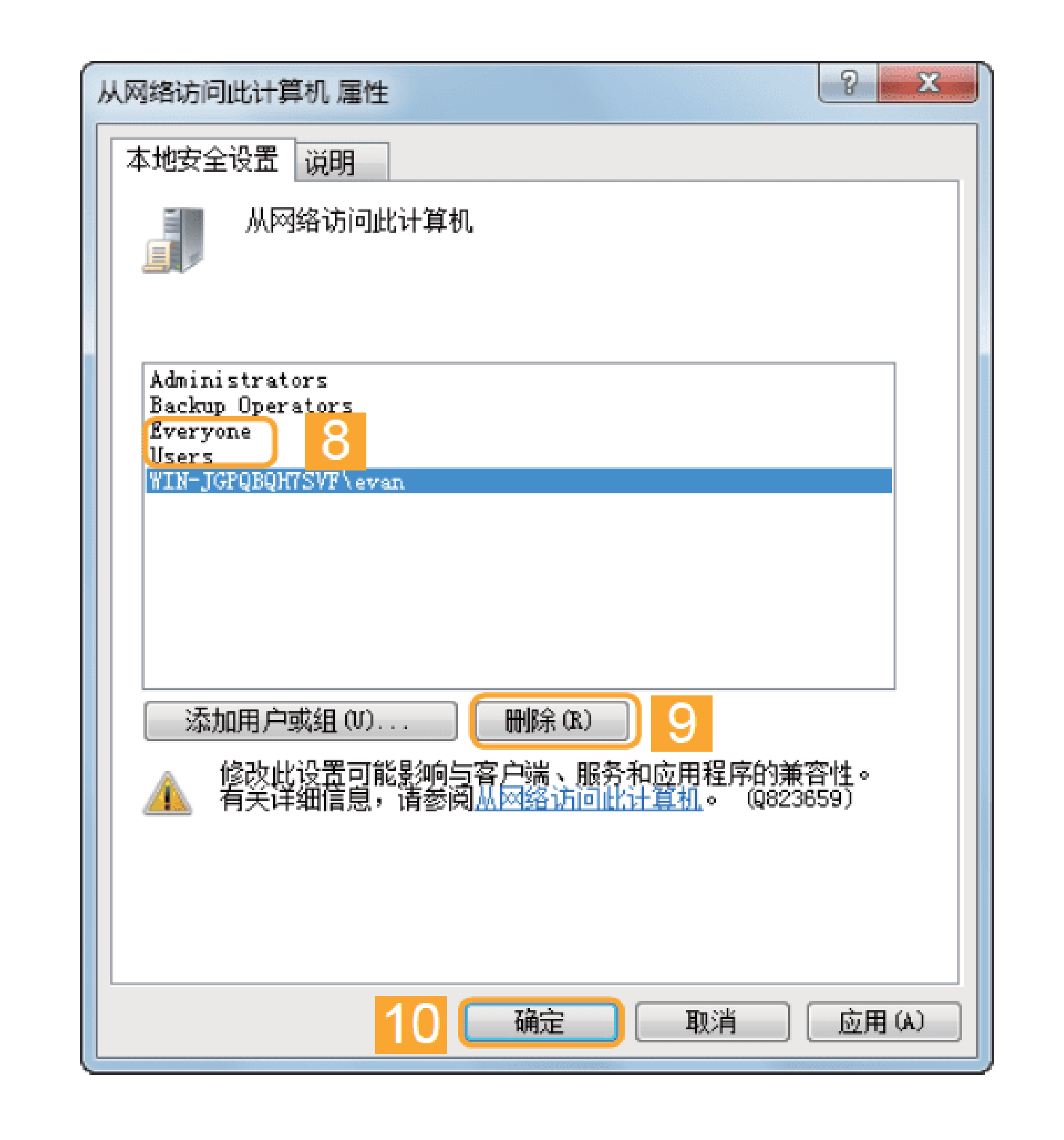
教你一招

输入名错误的将不显示用户对象

如果在“输入对象名称来选择”文本框中输入的用户名不存在，则单击检查名称(C)按钮后将打开对话框提示找不到此对象。

第5步：检查用户是否存在

返回“从网络中访问此计算机 属性”对话框，在其中的列表框中可查看到添加的用户名，然后分别选择Everyone和Users选项，单击删除(R)按钮删除用户，完成后单击确定按钮保存设置。



4.4 更进一步——限制他人使用电脑小秘招

通过阿伟的讲解，娜娜已经能够在自己的电脑中进行相关设置，让别人不能再轻易使用自己的电脑。但是她感觉这些设置太过复杂，想让阿伟教她一些简单有效的操作。阿伟很乐意为她讲解，于是娜娜又收集了一些简单的设置技巧。

第1招 设置账户的家长控制



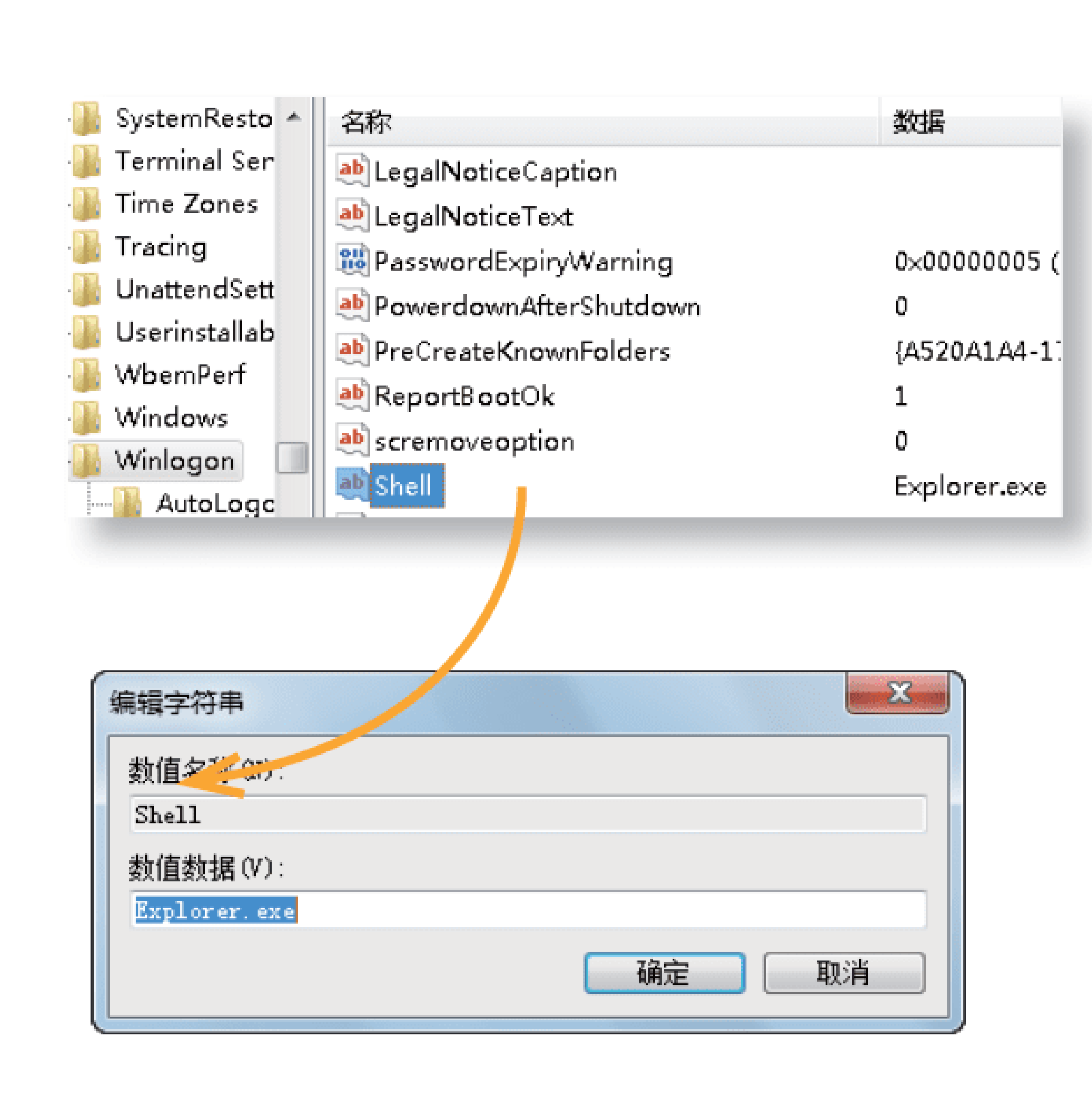
使用用户的家长控制能限制用户使用电脑的时间、访问电脑中的程序，其方法如下：

①打开“控制面板”窗口，然后单击“用户账户”超链接。

②在打开的窗口中单击“家长控制”超链接，打开“选择设置账户”窗口。

③在其中单击要设置家长控制的账户图标，在打开的窗口中选中“启用，应用当前设置”单选按钮，然后对当前账户的使用情况进行设置，完成后单击 确定 按钮。

第2招 登录系统桌面只显示背景图像



设置登录系统后，只显示背景图像，使他人访问电脑时不能进行任何操作，其方法如下：

①在“运行”对话框中执行**regedit**命令，打开注册表编辑器。

②在其左侧窗格中展开“HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon”选项，在右侧窗格中双击Shell选项。

③在打开对话框的“数值数据”文本框中将explorer.exe改成其他任意数值，单击 确定 按钮重启系统即可。

提示：要恢复桌面选项，在组策略中将Shell选项的“数值数据”还原为explorer.exe，打开任务管理器，选择“文件”/“新建任务”命令，在打开的对话框中新建explorer.exe进程，即可重新显示桌面项目。



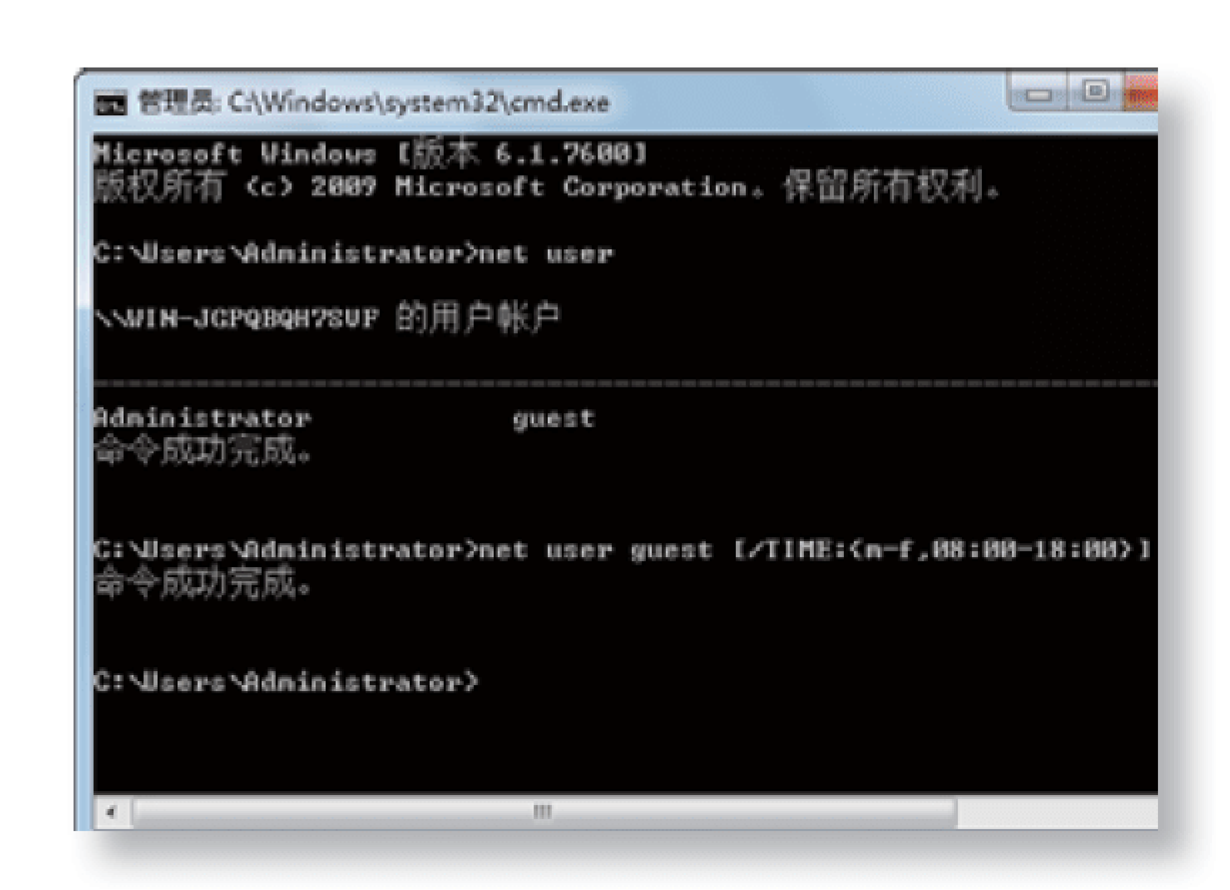
第3招 限制账户使用时间

在电脑中，为了方便易行，可在命令提示符中设置账户的使用时间以限制用户使用电脑，其方法如下：

①选择“开始”/“运行”命令，打开“运行”对话框。

②在其中输入“cmd”，按Enter键，打开命令提示符窗口。

③在命令提示符中输入“net user guest [/TIME:{m-f,08:00-18:00}]”，按Enter键执行命令即可限制该账户的使用时间。



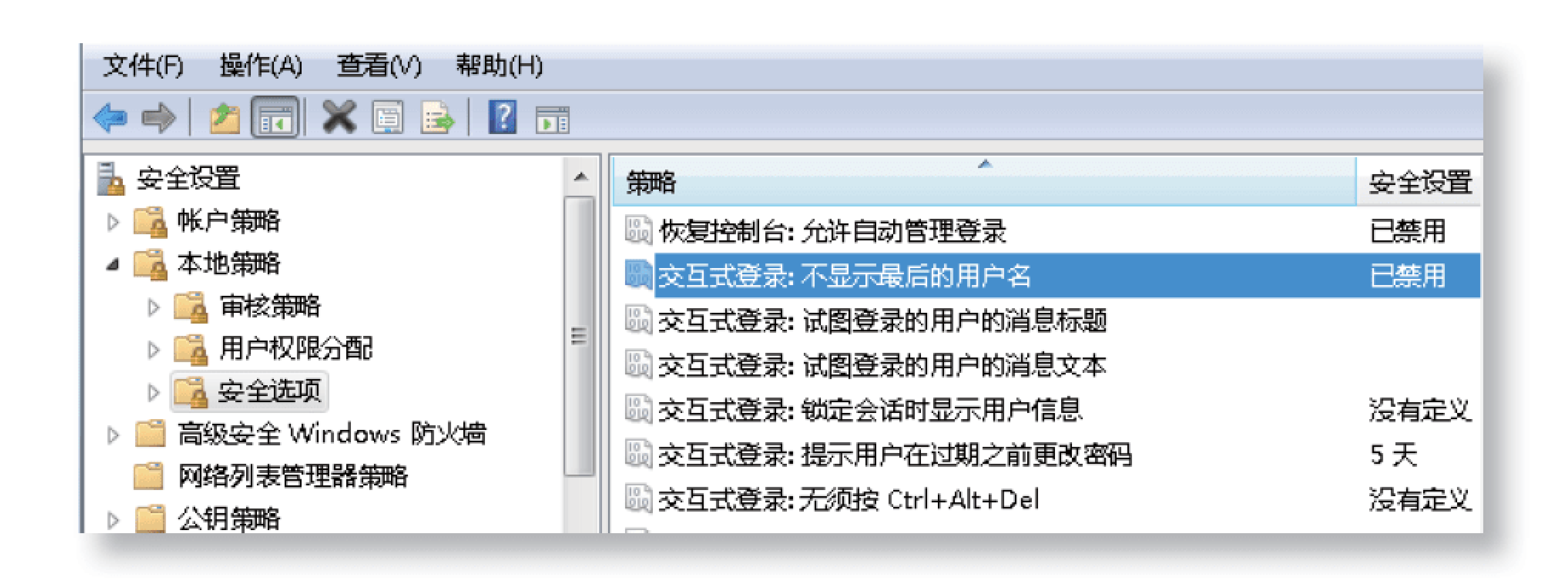
提示：在“net user guest[/TIME:{m-f,08:00-18:00}]”命令中，“guest”表示电脑中的用户账户，“m-f”表示此命令的有效时间是从星期一到星期五，“08:00-18:00”表示限制时间是从早8点到晚6点。

4.5 活 学 活 用

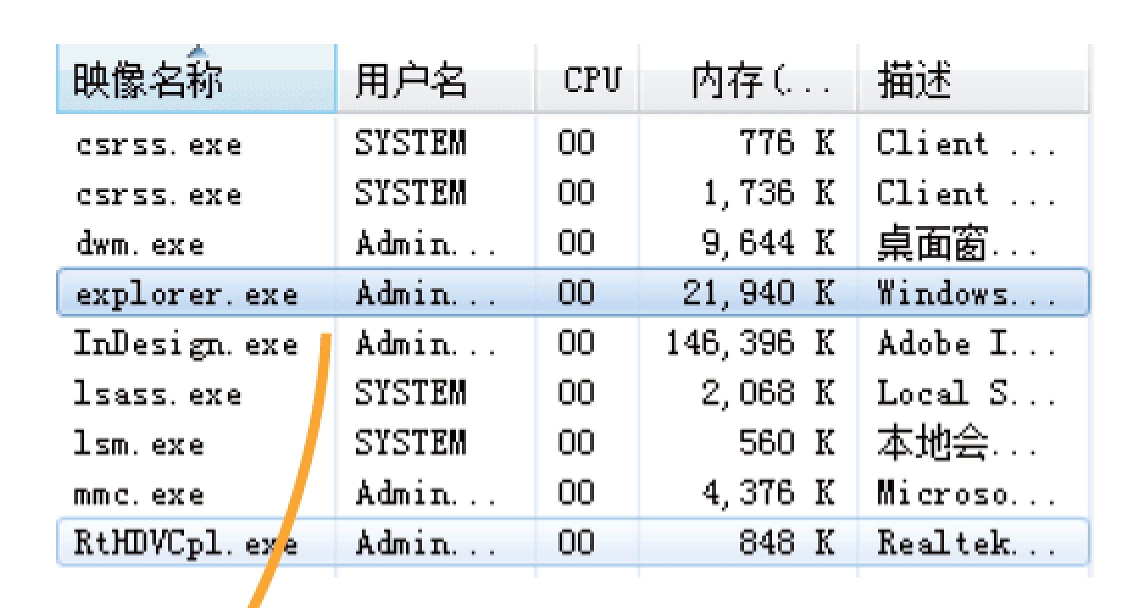
（1）列举限制他人使用电脑的方法，并简述其主要作用。

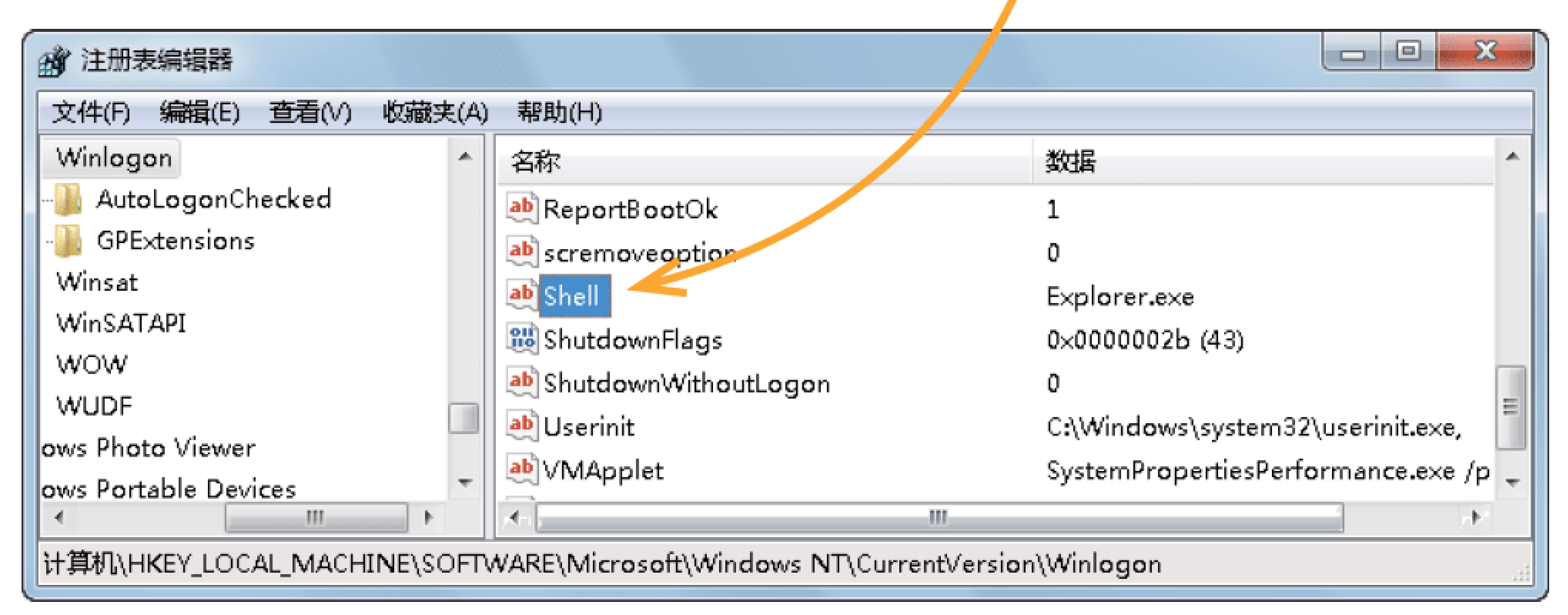
（2）根据学习的方法将电脑中的管理员账户和来宾账户进行重命名，然后创建另一个管理员账户。

（3）打开本地安全策略，在其中设置用户登录后重新启动电脑将不显示上次登录的账户名。



（4）结束explorer.exe进程，并在注册表中更改其Shell项的数值数据，使电脑在登录时只显示桌面背景，隐藏任务栏、开始菜单以及桌面上的图标。

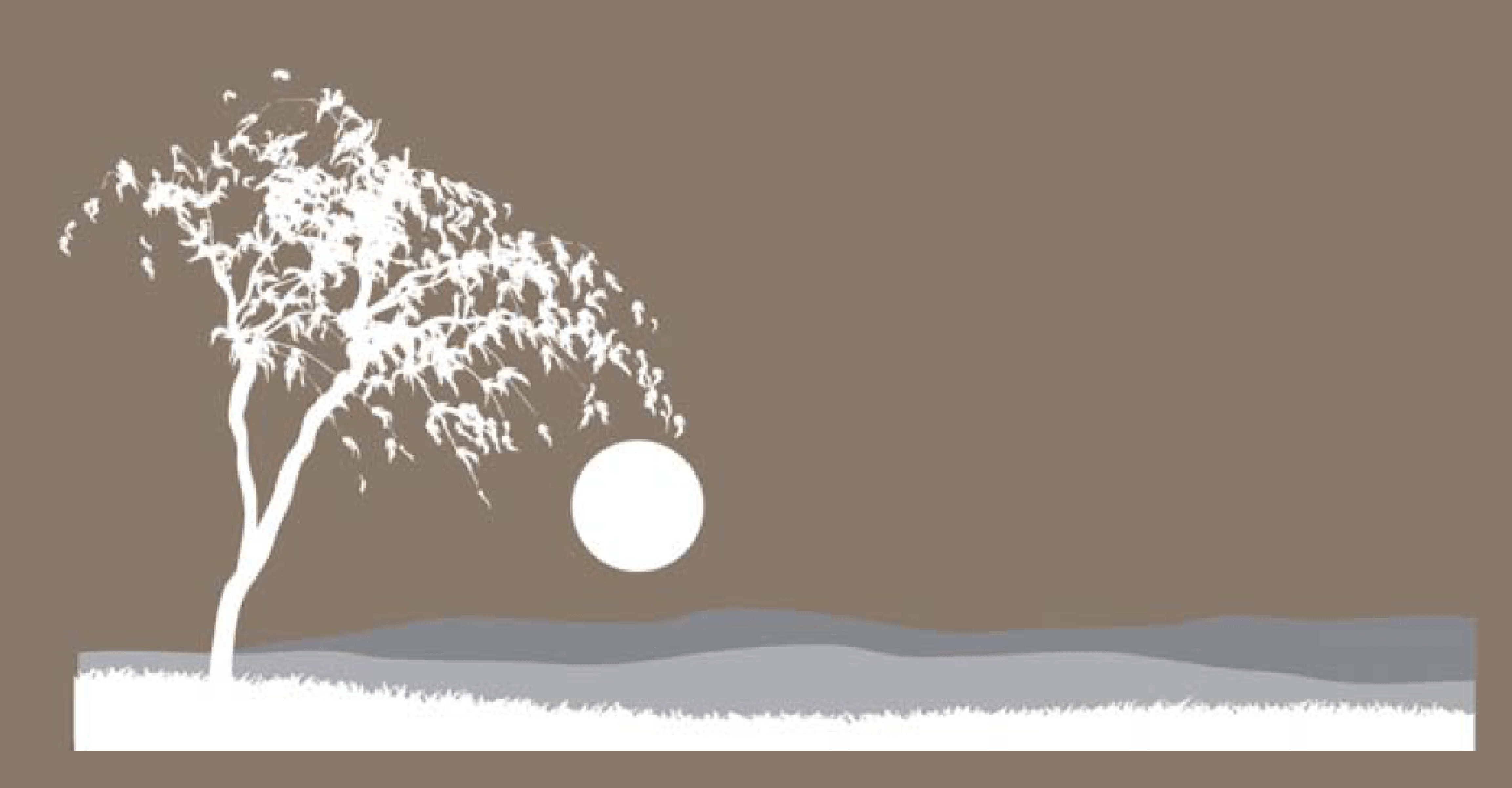




（5）在电脑中设置登录限制，如输入3次错误密码，将自动锁定电脑，半小时后才能再次输入账号和密码进行登录。



- ☑ 想知道系统漏洞是什么吗？
- ☑ 还在为系统中的使用权限太广泛而烦恼吗？
- ☑ 注册表能为操作系统安全做些什么？
- ☑ 想知道怎样让操作系统更安全吗？



第 05 章 打造安全操作系统很简单

娜娜早上刚打开电脑，就发现自己电脑桌面被改得面目全非，她很奇怪，“自己没有做这些变动啊，怎么就成这样了呢？”她找到阿伟求救，阿伟告诉她：“电脑的操作系统可能已经被破坏或感染了，别人利用漏洞侵入电脑，将你的组策略和注册表改动了。”娜娜听糊涂了：“漏洞、组策略和注册表这些都是什么啊？”好像有些印象，却又不知道在什么时候听过，于是，她要求阿伟为她详细地讲解。

5.1 系统漏洞的修复

娜娜问阿伟："系统漏洞是什么？"阿伟回答："简单地讲，系统漏洞就是操作系统存在的缺陷或后门，别人可以利用其非法进入电脑。"娜娜听了以后，感觉这很严重，马上催促阿伟为她想想办法防止这一安全隐患，阿伟笑着说："这是没有办法制止的，任何操作系统都会存在漏洞，我们可以对其进行修复，但不能够制止，我为你讲解了以后你就明白了。"

5.1.1 认识漏洞

通常将硬件、软件和协议的具体实现或系统安全策略上存在的缺陷称为漏洞，攻击者能够通过漏洞在未授权的情况下访问或破坏系统。那么，操作系统的漏洞是怎样定义和发现的呢?



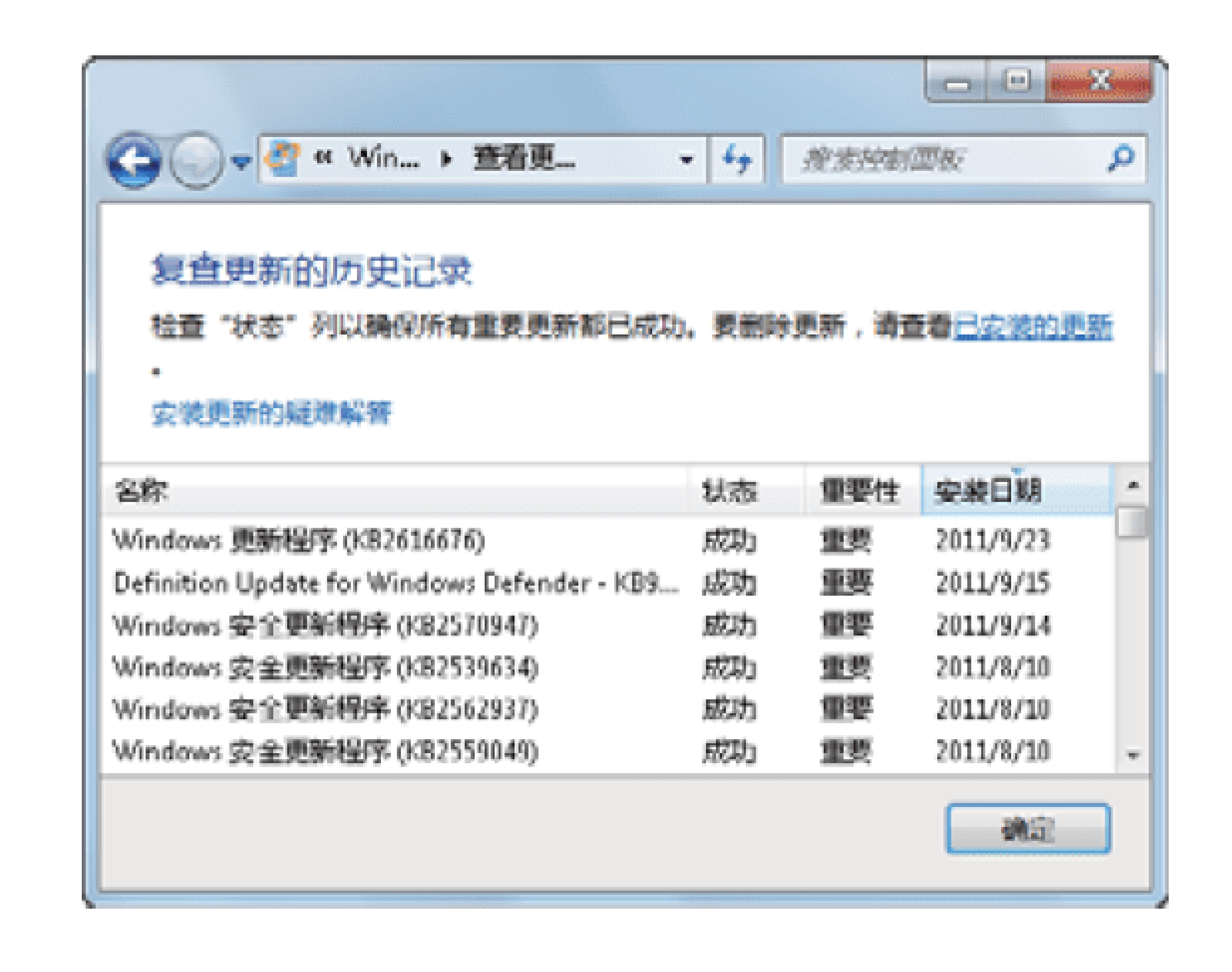
下面将分别对漏洞的定义和如何发现漏洞进行讲解。

1. 漏洞的定义

漏洞是指操作系统中存在的弱点或缺陷，对特定威胁攻击或危险事件的敏感性以及进行攻击的威胁作用的可能性。漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。这些缺陷、错误或不合理之处可能被有意或无意地利用，从而对一个组织的资产或运行造成不利影响。



提示：对于漏洞，从目前发现的漏洞情况来看，应用程序或软件中存在的漏洞远远多于操作系统中的漏洞，特别是网络应用中的漏洞更是占信息系统漏洞中的绝大多数。



2. 漏洞的发现

越早发现并修复漏洞，信息安全事件发生的可能性就越小。因此，漏洞发现是攻击者与防护者双方对抗的关键。使用专业漏洞扫描系统能自动检测远程或本地主机安全弱点的系统（如Windows自带的更新检查）。发现漏洞后，还要进一步通过自动或手动的漏洞验证来检验漏洞扫描结果的准确性。

5.1.2 新安装Windows系统中主要存在的漏洞

系统漏洞是病毒木马传播最重要的通道，不及时安装系统补丁的电脑，将无法阻止入侵。一个新装的Windows系统，需要安装的补丁可能多达上百个，其安全级别各有不同，那么，哪些是系统中必须修复的漏洞呢？



下面将介绍Windows 7中的部分高危漏洞和补丁名称，如下表所示。

Windows 7中的高危漏洞

漏 洞 类 型	补 丁 名 称
IE浏览器积累安全更新	KB2559049
Windows 7更新程序	KB2120976
Windows 更新程序	KB980423
IE浏览器CSS Oday漏洞	KB2416400
Mircosoft Office System安全更新	KB955936
Office远程代码执行漏洞	KB2289161
ActiveX Kill Bits积累安全更新	KB2562937
紧急安全更新Server 服务中的漏洞	KB958644



检测更多的系统高危漏洞

在电脑中安装360安全卫士，使用其“修复漏洞”功能可扫描出更多的系统高危漏洞，并对其安全级别进行分类，下载补丁进行修复。

5.1.3 了解漏洞与系统攻击的关系

随着互联网络的进步，操作系统中非法使用或破坏某一信息系统中的资源，以及非授权使系统丧失部分或全部服务功能的行为越来越严重，而其中涉及的系统漏洞以及相关的知识也较多，因此，它们之间的关系有重要的研究价值。



操作系统漏洞与系统攻击密切相关，主要包括如下几方面。

- **哪些才是安全漏洞：** 在系统具体实现和具体使用中产生的错误，但并不是系统中存在的错误都是安全漏洞。只有能威胁到系统安全的错误才是漏洞。许多错误在通常情况下并不会对系统安全造成危害，只有别人在某些条件下故意使用时才会影响系统安全。
- **系统安全漏洞的纠正过程：** 在实际使用中，首先发现系统中存在错误，而入侵者会有意利用其中的某些错误并使其成为威胁系统安全的工具，这时将确定这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。
- **系统攻击的条件：** 要对一个系统进行攻击，如果不能发现和使用系统中存在的安全漏洞是不可能成功的。对于安全级别较高的系统尤其如此，系统攻击者往往是安全漏洞的发现者和使用者。
- **攻击活动与安全漏洞紧密相关：** 不能脱离系统攻击活动来谈论安全漏洞问题。了解常见的系统攻击方法，对于有针对性的理解系统漏洞问题，以及找到相应的补救方法非常重要。

提示：要说明漏洞与系统攻击的关系，黑客是一个很好的实例，他们能有效地利用系统的安全漏洞对电脑进行攻击。



5.1.4 漏洞的分类

只要入侵者找到复杂的计算机网络中的一个漏洞，就能轻而易举地闯入系统。因此，了解这些漏洞可能存在的地方，对于修复它们有着重要的作用。



常见的系统漏洞主要包括软件编写存在的错误、系统配置不当和口令失窃等，下面将分别对其进行讲解。

1. 软件编写存在错误

在服务器程序、客户端软件或者操作系统中都存在错误，也就是只要是用代码编写的程序，都会存在不同程度的错误，其主要包括以下几种。

- 缓冲区溢出：入侵者在程序的有关项目中输入了超过规定长度的字符串，超过的部分通常就是入侵者想要执行的攻击代码，导致多出的攻击代码占据了输入缓冲区后的内存而执行。
- 多层代码使用问题：入侵者通常会利用操作系统多层代码的特点，在不同的层中输入窃取信息的代码进行入侵。
- 不对输入内容进行预期检查：编程人员对输入内容不进行预期的匹配检查，使入侵者输送炸弹的工作轻松简单。
- 文件操作的顺序以及锁定：入侵者利用处理顺序上的漏洞改写某些重要文件从而达到闯入系统的目的，所以，编程人员要注意文件操作的顺序以及锁定等问题。

2. 系统配置不当

系统的配置对系统的安全非常重要，如果对系统的配置信息不做严格的处理，将造成系统的漏洞。

- 默认配置的不足：系统在安装后都有默认的安全配置信息，通常这种配置信息将给入侵者提供入侵依据。
- 管理员疏忽：系统安装后没有对管理员口令进行密码的设置。入侵者首先要做的事情就是搜索网络上没有密码的电脑。
- 临时端口：管理员如果在电脑中打开一个临时端口作为测试端口，但测试完后却忘记了禁止它，这样就会给入侵者有机可乘。
- 信任关系：网络间的系统经常建立信任关系以方便资源共享，但这也给入侵者带来了攻击的可能。

3. 口令失窃

入侵者能对简单的口令进行轻易地破解，也可以使用程序工具进行攻击，窃取用户名和密码。

- **简单的口令：** 如果将管理员口令设置得过于简单，入侵者就可轻易地进行破解。
- **字典攻击：** 入侵者使用一个程序借助一个包含用户名和口令的字典数据库，不断地尝试登录系统，直到成功进入。这种方式的关键在于有一个好的字典。
- **暴力攻击：** 与字典攻击类似，但这个字典却是动态的，包含了所有可能的字符组合。

新手解惑

Q：漏洞的分类还包括哪些？

A：除此之外，漏洞还包括入侵者在网络上放置一个嗅探器，就可以查看该网段上的通信数据以及系统设计的缺陷（TCP/IP缺陷）。

5.1.5 使用360安全卫士修复漏洞

为了防止黑客等入侵者利用系统漏洞攻击电脑，用户可将系统存在的高危漏洞进行修复。



下面将使用360安全卫士修复漏洞，其具体操作如下。



第1步：扫描漏洞

启动360安全卫士，选择“修复漏洞”选项卡，系统将自动扫描漏洞，并将扫描的漏洞信息显示在下方的列表框中。



提示：扫描完成后，可单击 重新扫描 按钮重新进行扫描，以准确地检测出系统中存在的高危漏洞。

第2步：修复漏洞

扫描完成后，单击 立即修复 按钮即可下载补丁程序对系统漏洞进行修复，修复完成后，将提示该漏洞已修复。

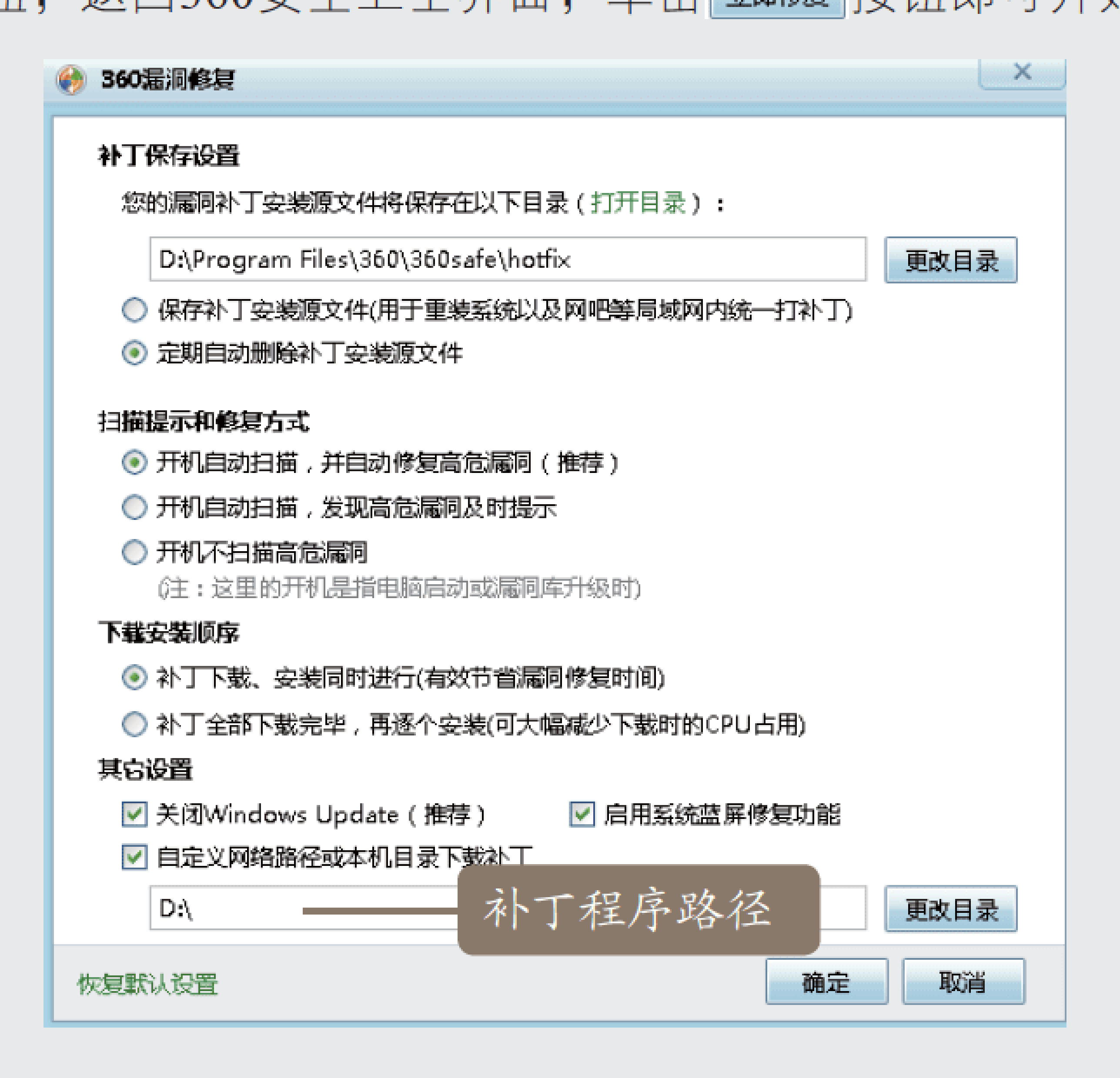


提示：使用360安全卫士修复系统漏洞时，软件将选择性地修复，对于与该系统或电脑有冲突的补丁程序将忽略不进行安装。

教你一招

如何在无网络的情况下使用已有的补丁程序进行修复漏洞

在360安全卫士中的“修复漏洞”选项卡中单击“设置”超链接，在打开的“360漏洞修复”对话框的“其他设置”栏中选中“自定义网络路径或本机目录下载补丁”复选框，在其下方的文本框中设置其补丁程序的位置，单击 确定 按钮，返回360安全卫士界面，单击 立即修复 按钮即可开始修复。



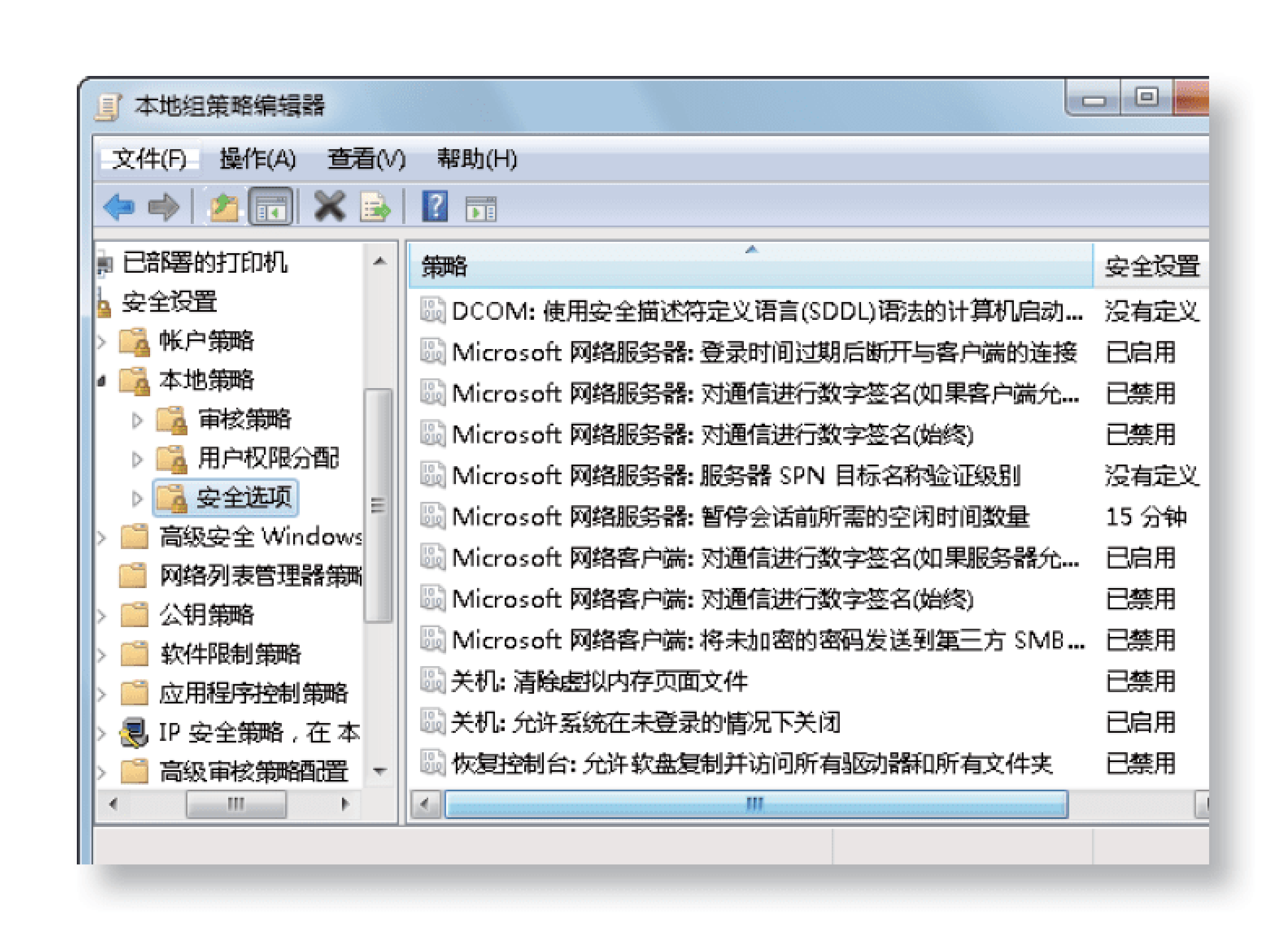
5.2　系统组策略安全设置

在为娜娜讲解了漏洞的修复后，阿伟看娜娜好像还意犹未尽，于是问她：“你现在应该对漏洞有所了解了吧？”娜娜回答道：“很简单嘛，我只要使用360安全卫士就可以解决所有的问题了。”随后，阿伟就开始为她讲解组策略的知识，并且提醒她一定要认真学习，因为组策略在很多地方都可以使用。

5.2.1　认识组策略

很多人感觉组策略很神秘，也很难懂，其实组策略主要用于管理员为用户和电脑定义并控制程序、网络资源及操作系统行为。通过使用组策略可以设置各种软件、电脑和用户策略。

组策略可以帮助系统管理员针对整个电脑或是特定用户来设置多种配置，包括桌面配置和安全配置。如系统中有多个用户，可以为将要限制的用户或用户组设置可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个系统范围内创建特殊的桌面配置。可以认为组策略是Windows中的一套系统更改和配置管理工具的集合。



新手解惑

Q：Windows 7中有更好的安全保障吗？

A：通过使用组策略可以设置各种软件、电脑和用户策略。考虑到安全方面的原因，Windows 7已经开发了许多新的和增强的组策略功能和服务，能够更好地保护电脑中的数据、功能和服务。

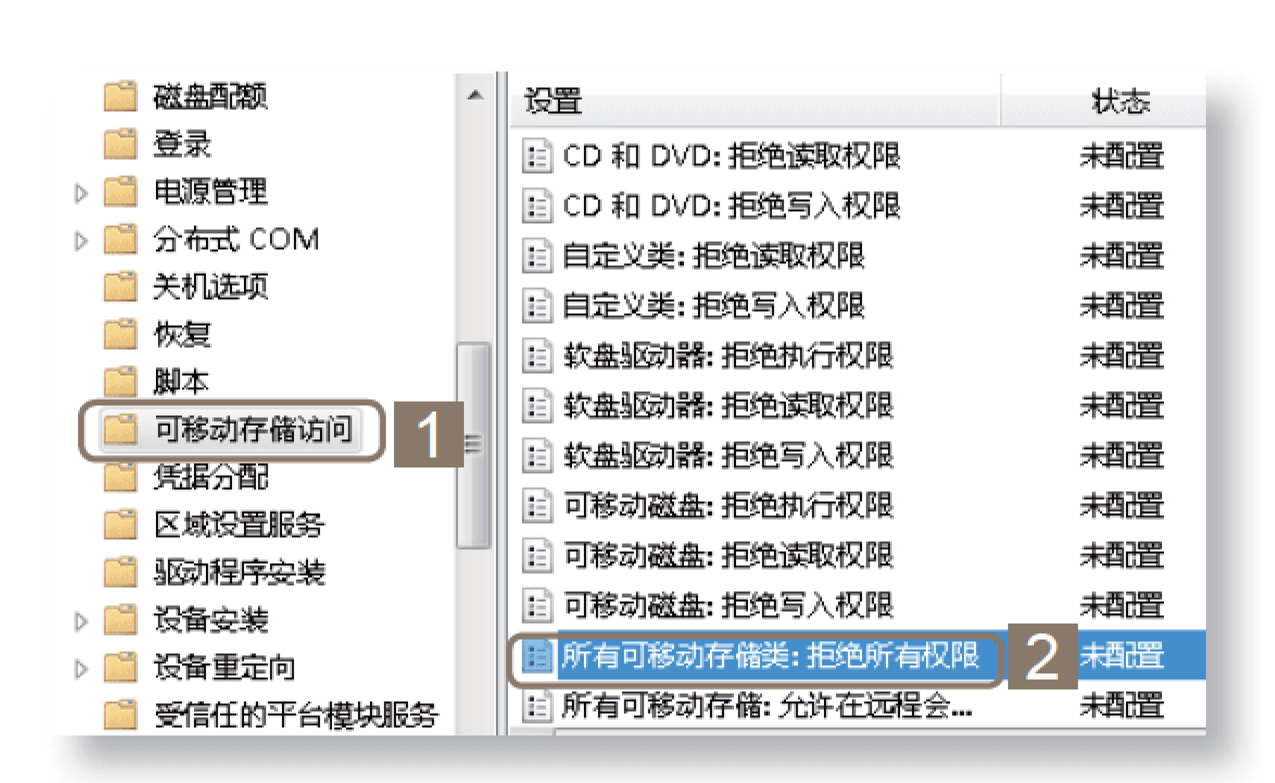


5.2.2 禁止使用U盘

在操作系统中为了防止使用U盘传输数据而使电脑感染病毒，威胁操作系统的安全，可以通过组策略禁止在电脑中使用U盘。



选择“开始”/“运行”命令，在打开的“运行”对话框中输入“gpedit.msc”，然后按Enter键，打开组策略编辑器，在其中即可进行设置，其具体操作如下。

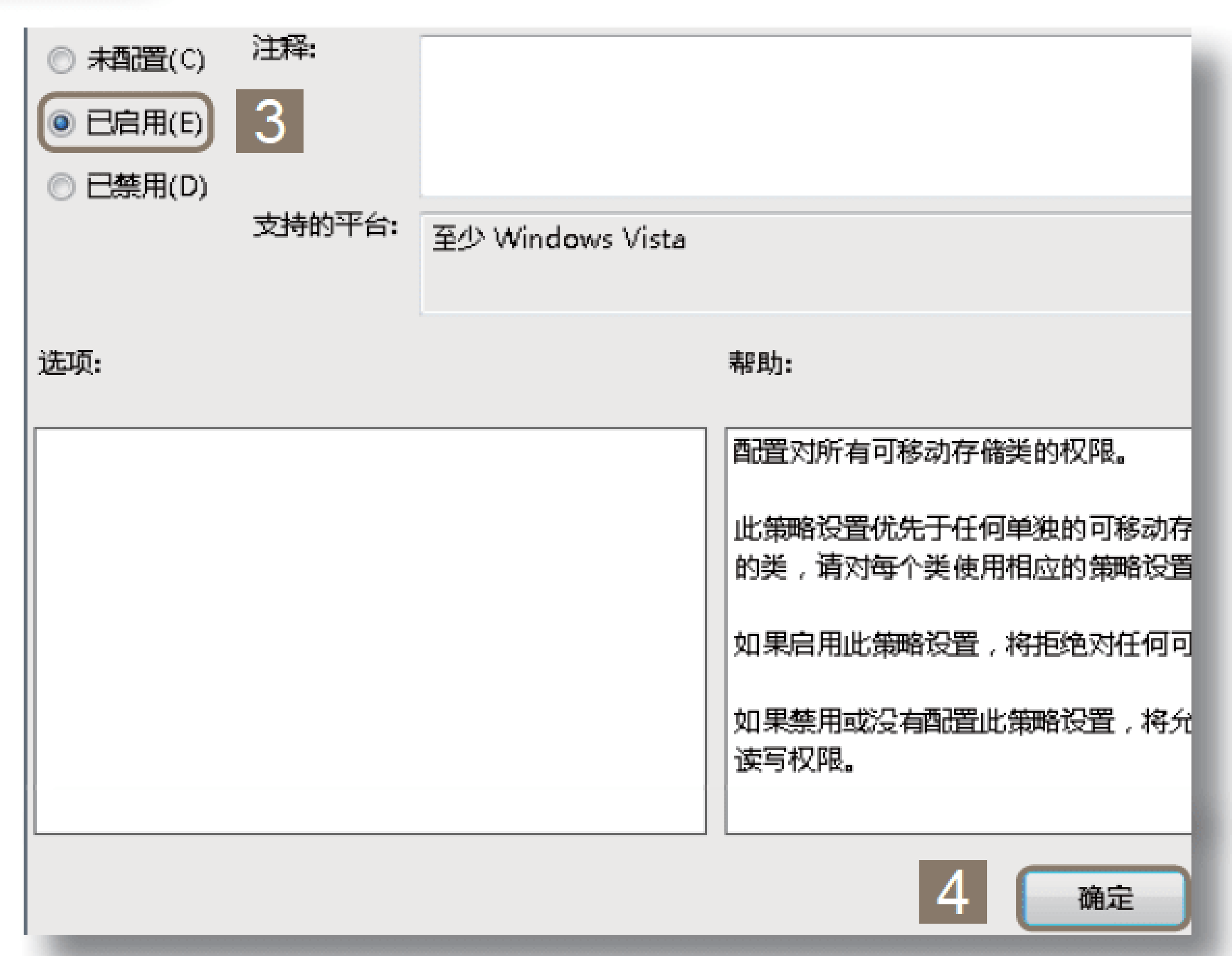


第1步：打开配置对话框

在组策略编辑器左侧窗格中依次展开“计算机配置/管理模板/系统/可移动存储访问”选项，在右侧窗格中双击“所有可移动存储类:拒绝所有权限”选项，打开目标策略属性设置对话框。

第2步：启用安全策略

在“所有可移动存储类:拒绝所有权限”对话框中选中“已启用”单选按钮，单击确定按钮完成配置，此时就可以完全禁止USB存储类设备。



教你一招

禁止使用U盘读取和写入数据

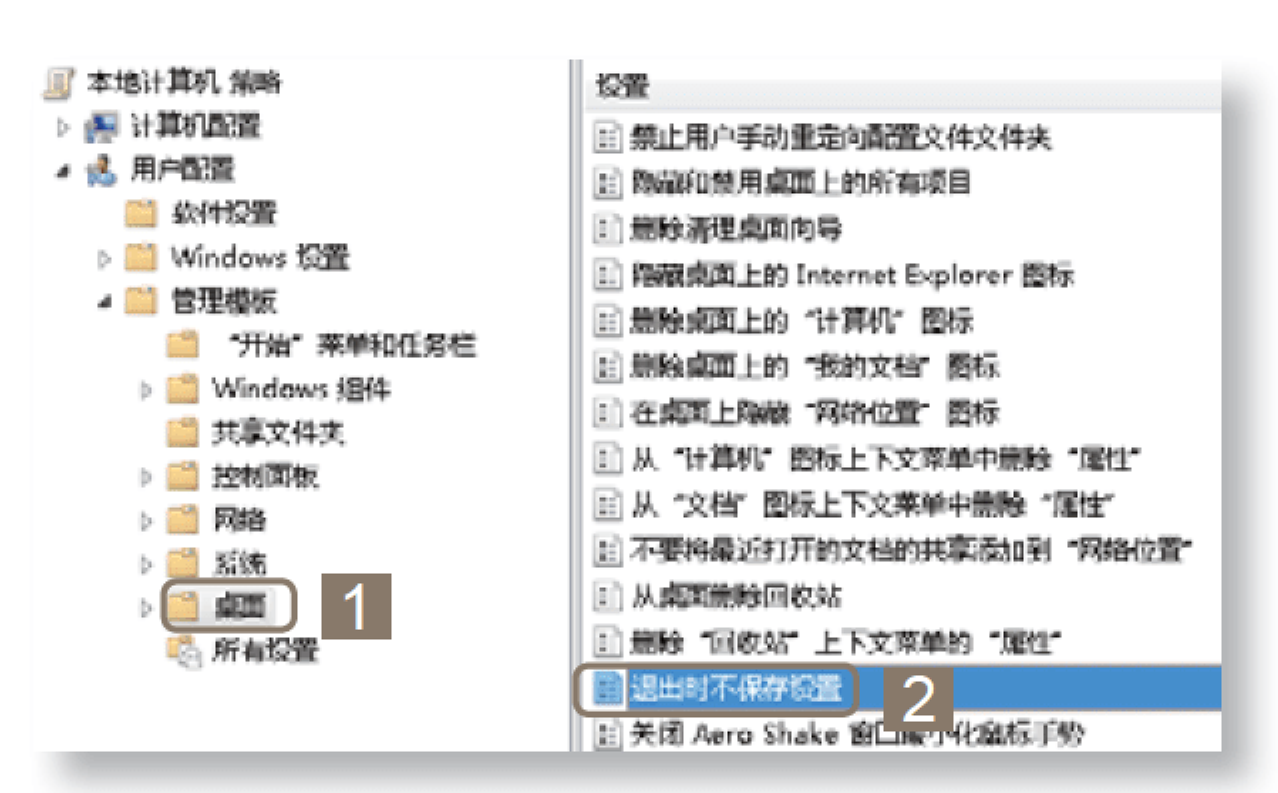
在“可移动存储访问”选项中，可对移动存储介质的读取和写入权限作禁止设置，其方法为：分别在右侧窗格中双击“可移动磁盘:拒绝读取权限”和“可移动磁盘:拒绝写入权限”选项，在打开的对话框中启用该配置即可。

5.2.3 禁止更改桌面设置

在操作系统中如果不希望别人对其桌面进行修改，可通过隐藏桌面图标和退出时不保存桌面设置实现。这样既保护了系统的安全性，又能使用户的桌面不能随意被修改。



下面将对在组策略中禁止更改桌面设置进行设置，其具体操作如下。



第1步：选择“退出时不保存设置”选项

打开本地组策略编辑器，在其左侧窗格中依次展开“用户配置/管理模板/桌面”选项，在其右侧窗格中双击“退出时不保存设置”选项，打开其配置对话框。



第2步：启用配置

在打开的对话框中选中“已启用”单选按钮，单击 确定 按钮启用配置，完成后系统将在退出时不保存对桌面的相关设置，如打开窗口的位置，任务栏的大小和位置等。



第3步：隐藏桌面图标

在展开的选项中双击“隐藏桌面上的Internet Explorer图标”选项，在打开的对话框中选中“已启用”单选按钮，单击 确定 按钮启用该配置。使用相同的方法分别隐藏桌面上的网络位置、计算机、回收站以及我的文档等图标，即可实现禁止桌面设置不被修改。



5.2.4 禁止访问控制面板

通过控制面板可以对操作系统的重要选项进行设置，如添加与删除程序、用户账户以及管理工具等，这些设置严重影响了操作系统的安全，因此，可通过禁止访问控制面板来保证操作系统的安全。



下面将对组策略中设置禁止访问控制面板的方法进行讲解，其具体操作如下。



第1步：选择禁止访问控制面板

打开本地组策略编辑器，在其左侧窗格依次展开"用户配置/管理模板/控制面板"选项，在其右侧窗格中双击"禁止访问'控制面板'"选项，打开配置对话框。



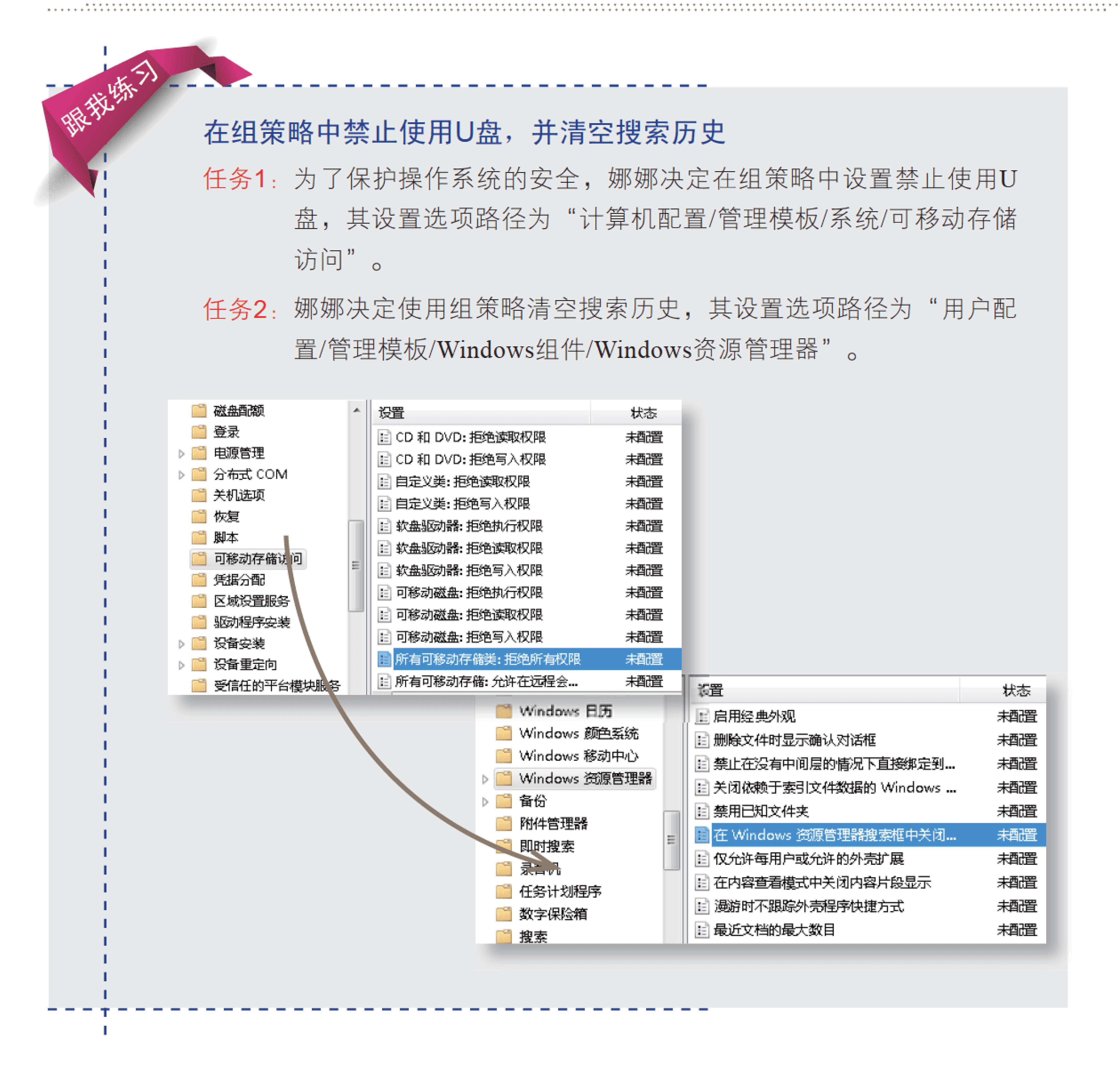
第2步：禁止访问控制面板

在打开的对话框中选中"已启用"单选按钮，然后单击 确定 按钮启用配置，设置完成后，在"开始"菜单中将隐藏控制面板。

教你一招

如何取消组策略中的设置

对于在组策略中设置了的选项，如果要还原到设置前的效果，可重新打开该选项对应的对话框，在其中选中"已禁止"单选按钮，单击 确定 按钮完成。



在组策略中禁止使用U盘，并清空搜索历史

任务1：为了保护操作系统的安全，娜娜决定在组策略中设置禁止使用U盘，其设置选项路径为“计算机配置/管理模板/系统/可移动存储访问”。

任务2：娜娜决定使用组策略清空搜索历史，其设置选项路径为“用户配置/管理模板/Windows组件/Windows资源管理器”。

5.3　注册表安全设置

阿伟告诉娜娜，注册表可以控制控制面板功能、桌面外观和图标、网络参数以及浏览器功能和特征等，因此，对注册表的设置能影响操作系统的正常使用。娜娜听了阿伟的介绍以后，便要求阿伟给她讲解注册表的设置。

5.3.1　认识注册表

用户在准备运行一个应用程序时，注册表将提供应用程序信息给操作系统，这样应用程序才可以被找到，因此，注册表是用来存储操作系统中应用程序相关设置的场所。

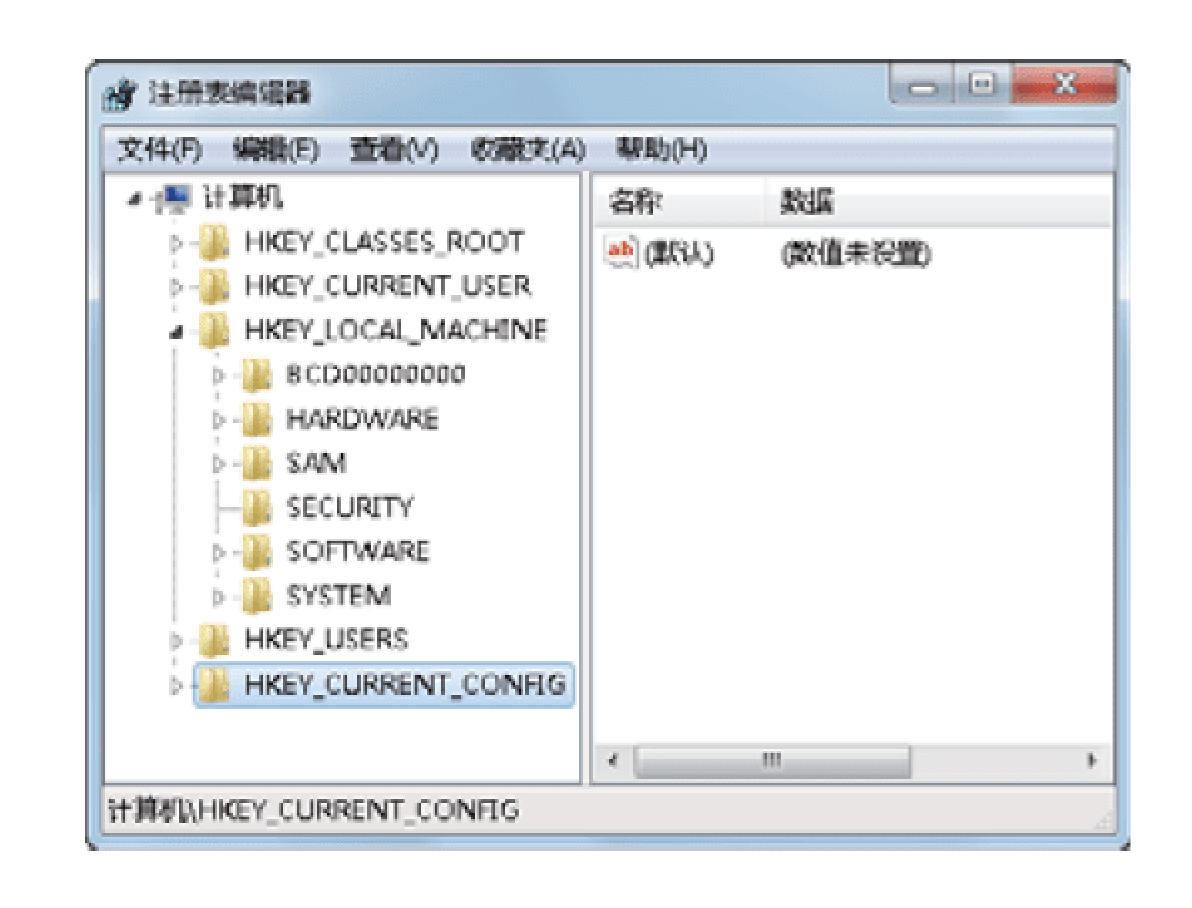




下面将对注册表的简介、注册表的作用以及注册表的启动方法进行讲解。

1. 注册表的简介

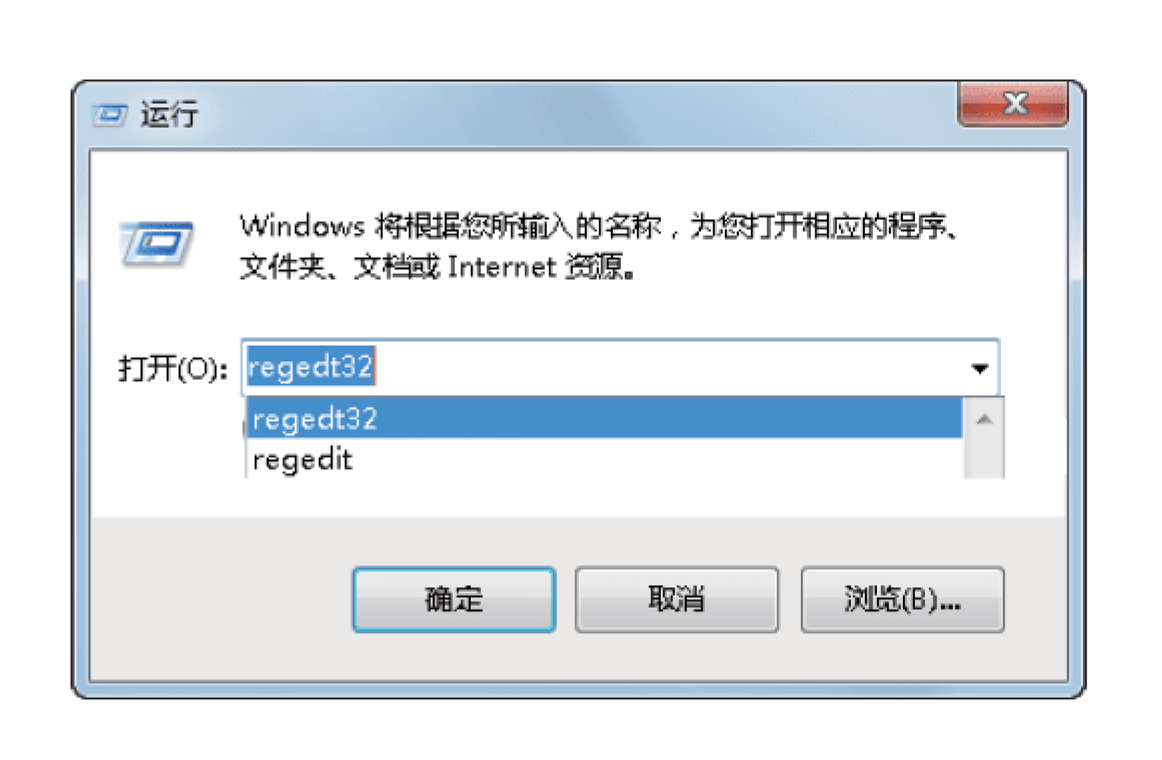
注册表是Windows程序员创建的一个多层次式且不同系统中基本结构相同的信息数据库。电脑配置和默认用户设置的注册表数据被保存在DEFAULT、SAM、SECURITY、SOFTWARE、SYSTEM和NTUSER.DAT 6个文件中。



2. 注册表的作用

在操作系统中，注册表控制所有应用程序和驱动，并且是基于用户和电脑系统，而不依赖于应用程序或驱动，每个注册表的参数项控制了一个用户的功能或者计算机功能。用户功能可能包括了桌面外观和用户目录。系统功能和安装的硬件和软件有关，因此，对所有用户都是公用的。





3. 注册表的启动方法

启动注册表很简单，可通过在“运行”对话框中输入命令进行启动，其方法为：选择“开始”/“运行”命令，打开“运行”对话框，在其中输入“regedit”或者“regedit32”，按Enter键即可。

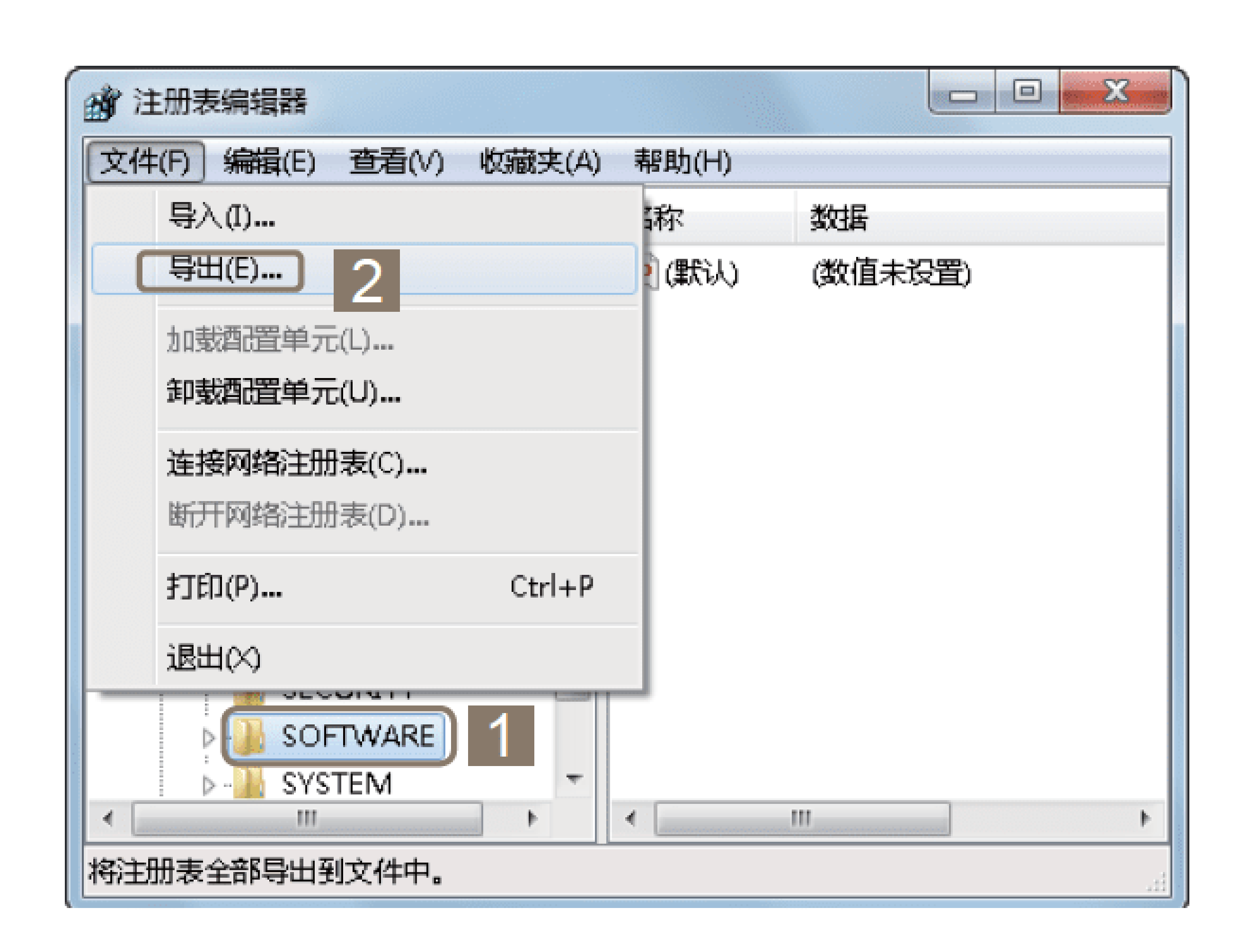
提示：输入“regedit32”，在打开的注册表编辑器中可方便地设置权限。建议网络管理员使用这种方法打开注册表编辑器，修改需要修改的权限设置部分防止被他人恶意修改。

5.3.2 备份和还原注册表

通常情况下，软件程序会自动更改注册表，用户无须对注册表做不必要的更改。对注册表进行错误更改会导致 Windows 停止运行或报错。因此，进行任何更改前需备份注册表。如果系统变得不稳定，硬件停止运行，或者在对注册表进行编辑后，软件无法运行时可将备份的注册表还原。



下面将对注册表的备份和还原进行讲解，其具体操作如下。



第1步：选择备份对象

打开注册表，在其中选择要备份的选项，这里选择SOFTWARE选项，然后选择“文件”/“导出”命令。

提示：如果想要备份某个特定项或子项，可选择要备份的项或子项。

第2步：保存文件

在打开对话框的“保存在”下拉列表框中设置要保存的位置，在“文件名”下拉列表框中输入“SOFTWARE”，然后单击 保存(S) 按钮即可完成保存。



教你一招

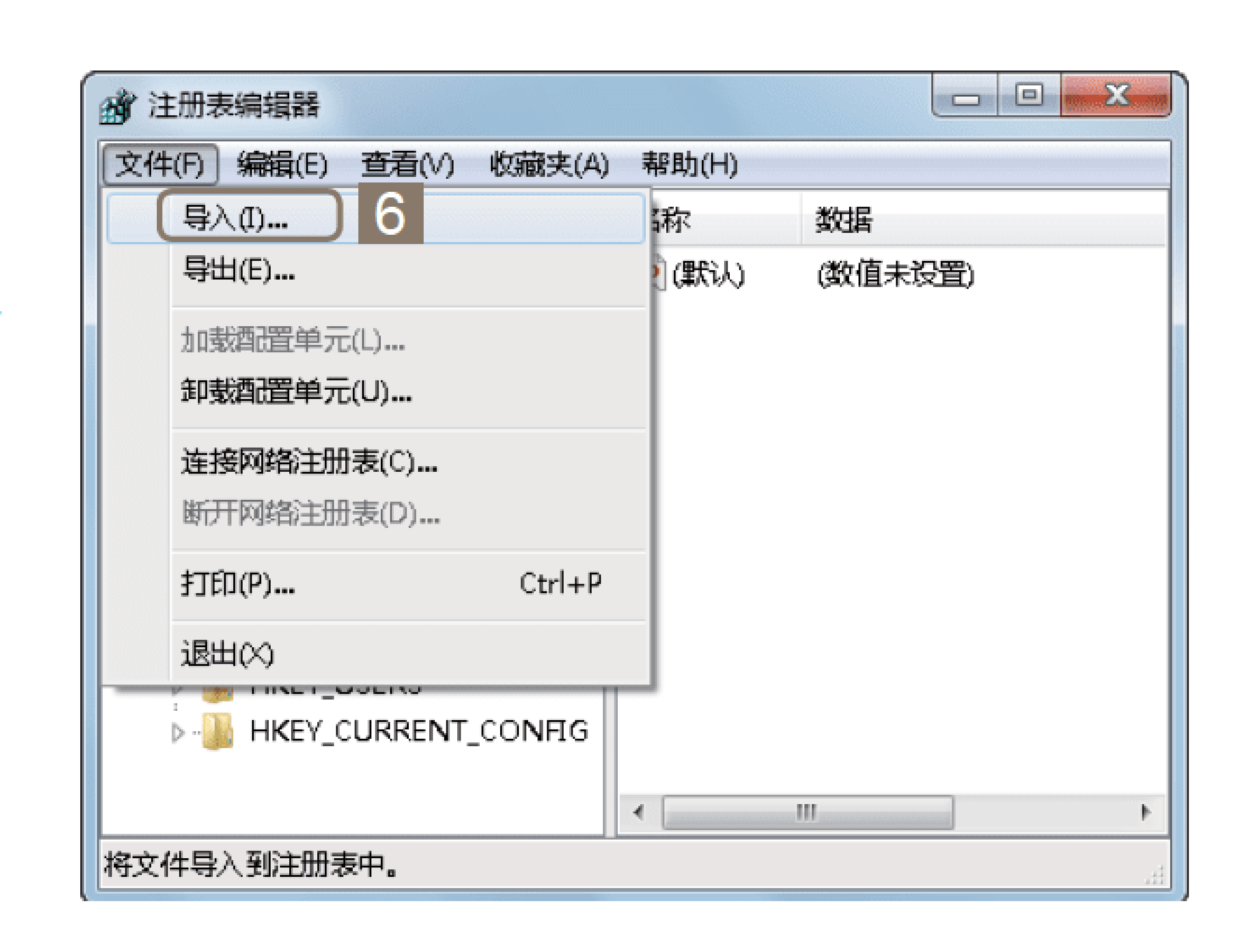
备份整个注册表

如果要备份整个注册表，可在注册表左侧窗格中选择“计算机”选项，然后使用相同的方法即可对整个注册表进行备份。



第3步：选择还原对象

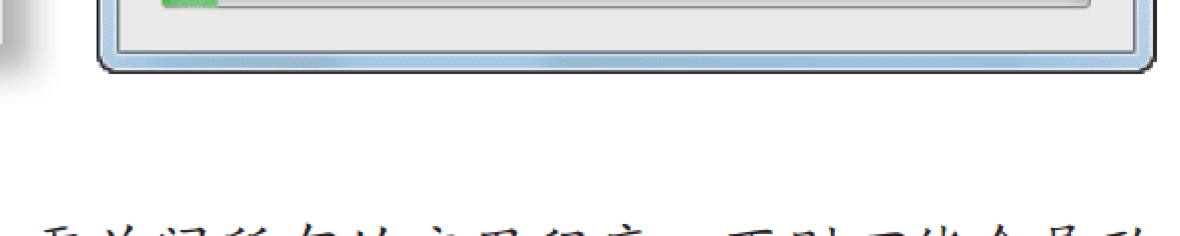
在电脑出现因注册表出错导致的问题后，可打开注册表进行还原，选择注册表中要进行还原的选项，这里选择SOFTWARE选项，然后选择“文件”/“导入”命令。



提示：如要还原整个注册表，可在注册表的左侧窗格中选择“计算机”选项。

第4步：还原注册表文件

在打开的对话框中找到并选中备份文件，然后单击“打开(O)”按钮，系统将打开“导入注册表文件”对话框，显示导入进度。



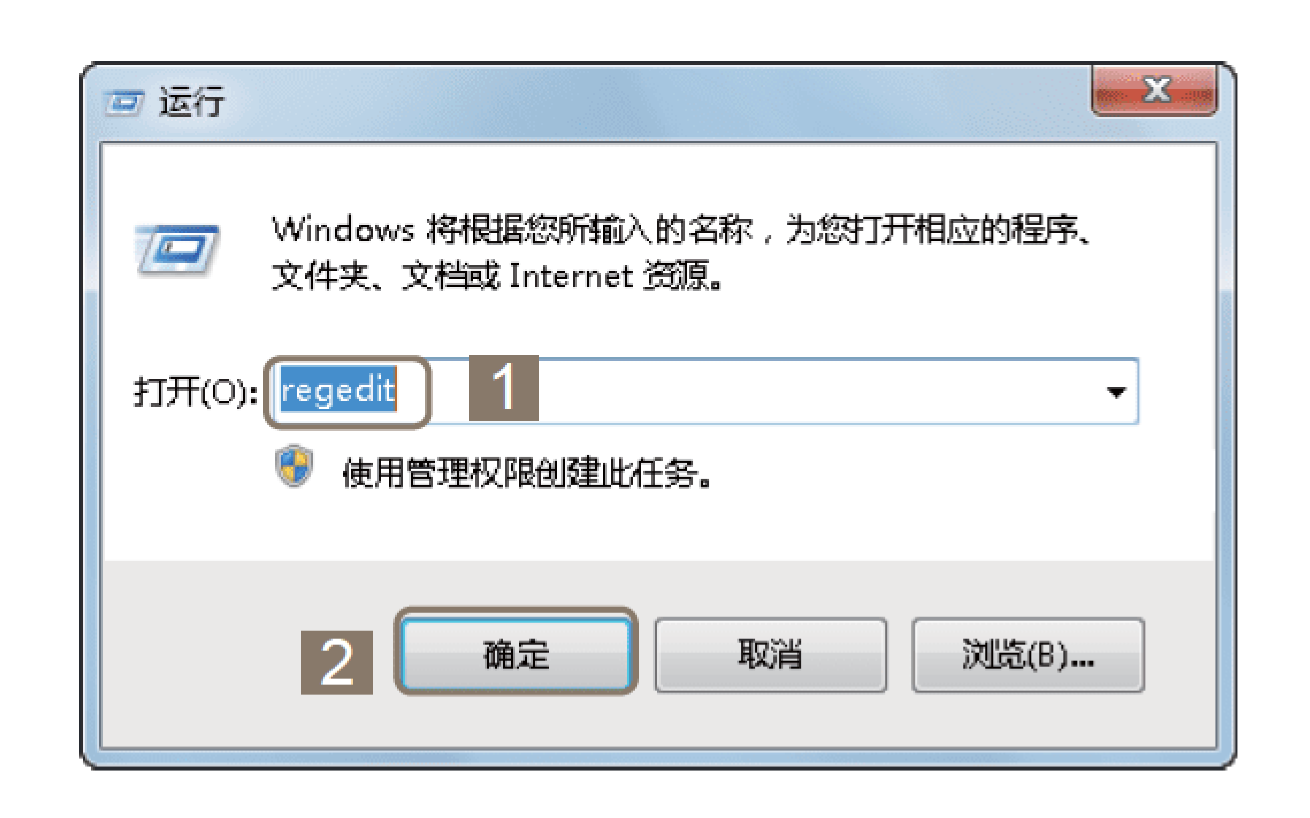
提示：在对注册表进行备份或还原时，需关闭所有的应用程序，否则可能会导致备份或还原不完善。

5.3.3　禁止危险的启动项

系统中的启动项过多不仅会导致电脑开机缓慢，而且在这些启动项中还可能包含病毒，这不仅会影响系统的运行，还会导致电脑出现安全问题。这时，可在注册表中删除不需要的启动项目以解决此问题。



下面将对在注册表中删除危险启动项进行讲解，其具体操作如下。



第1步：打开注册表

选择“开始”/“运行”命令，打开“运行”对话框，在其中的文本框中输入“regedit”，单击确定按钮打开注册表。

第2步：删除不必要的启动项

在注册表左侧窗格中依次展开HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run选项，在右侧窗格中要删除的选项上单击鼠标右键，在弹出的快捷菜单中选择“删除”命令即可。



5.3.4　禁止远程修改注册表

网络中的电脑可以远程对注册表进行更改，一方面可方便用户对电脑的控制，另一方面却威胁了电脑的安全。注册表的改变将影响操作系统的正常使用，恶意的修改还会破坏操作系统的稳定性。



下面将对通过修改注册表禁止远程修改注册表进行介绍，其具体操作如下。

第1步：新建选项

打开注册表编辑器，在其左侧窗格依次展开HKEY_LOCAL_MACHINE/System/Current ControlSet/Control/SecurePipeServers/winreg选项，在右侧窗格中单击鼠标右键，在弹出的快捷菜单中选择“新建”/“DWORD（32位）值”命令。





第2步：设置新建项

在新建的选项上单击鼠标右键，在弹出的快捷菜单中选择“重命名”命令，输入“RemoteRegAccess”，按Enter键确认输入。然后双击该选项，在打开对话框的“数值数据”文本框中输入“1”，然后单击确定按钮即可。

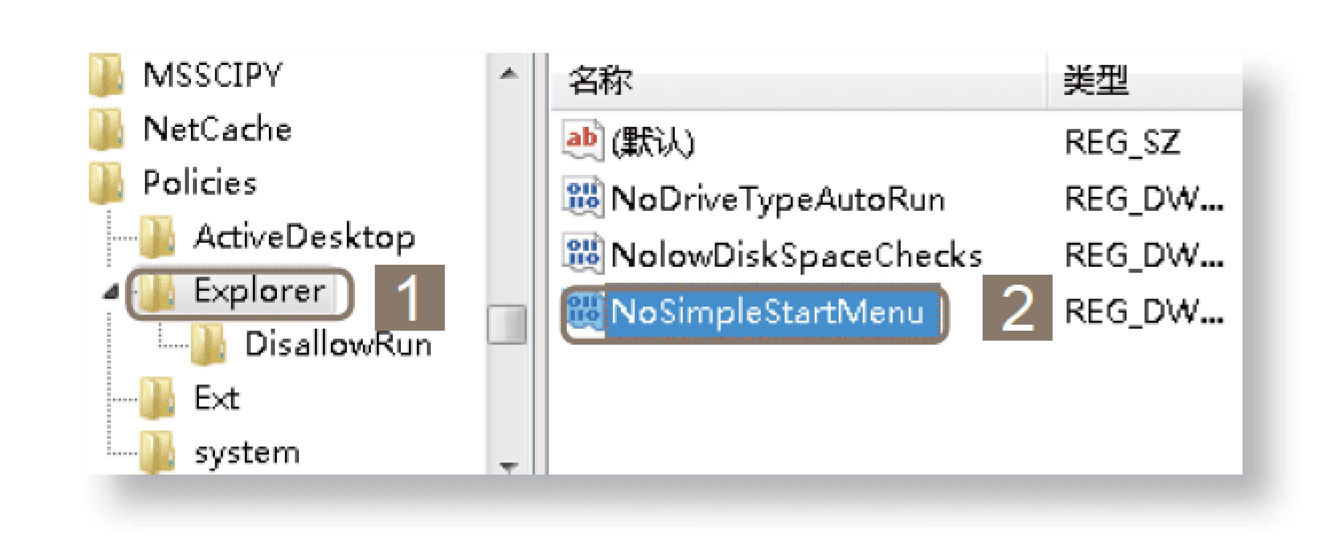


5.3.5 禁止使用“开始”菜单

如果用户仅使用电脑中的一些简单的程序，可以直接使用桌面上的快捷方式，禁用其“开始”菜单防止电脑的相关设置被修改，在注册表中可以通过修改其中的数值达到禁用“开始”菜单的目的。



下面将对禁用“开始”菜单的方法进行讲解，其具体操作如下。



第1步：新建NoSimpleStartMenu值

打开注册表编辑器，在其左侧窗格中依次展开HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer选项，在右侧新建DWORD值项NoSimpleStartMenu，然后双击该选项。

教你一招

禁用“开始”菜单中的“运行”选项

在HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/Policies/Explorer项中添加值为1的NoRun选项，即可禁用“运行”命令。

第2步：设置新建项数值数据

在打开对话框的“数值数据”文本框中输入“1”，然后单击确定按钮即可。

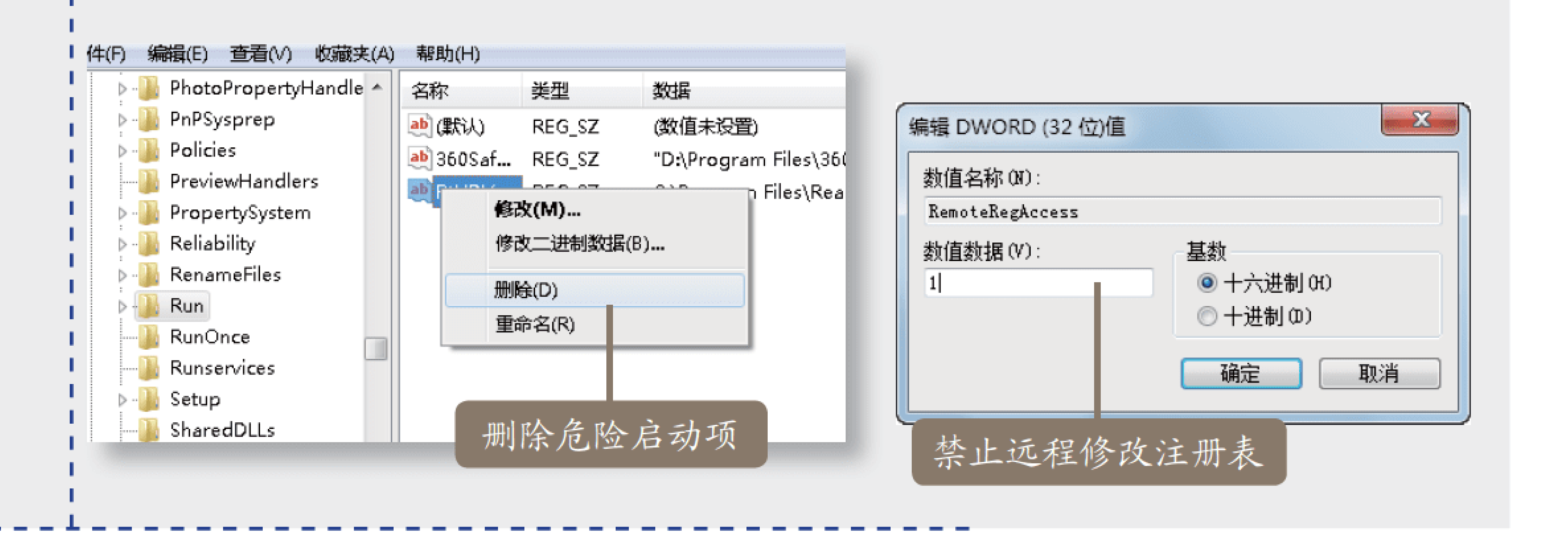


跟我练习

打开注册表，通过修改其中的数值禁止危险的启动项及远程修改注册表

任务1：在注册表中展开HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run选项，将其中多余的启动项删除。

任务2：在注册表中展开HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/SecurePipeServers/winreg选项，在其中添加RemoteRegAccess选项，并将其数值数据设置为1。



5.4 操作系统的其他安全技术

阿伟在为娜娜讲解了组策略和注册表的安全设置后，感觉这些对于娜娜来说实在是有点困难，需要慢慢地理解和消化才能掌握。为了加深娜娜对操作系统安全的理解，阿伟决定再为娜娜讲解一些关于操作系统的安全保护的知识。娜娜对阿伟的想法很赞同，于是又接着跟阿伟开始学习。



5.4.1 开启审核功能

使用本地安全策略能对电脑的相关安全选项进行配置，在其中开启审核功能可以记录攻击者的入侵企图，用户可通过这些痕迹采取相应的防范措施并对攻击者进行追踪，因此，该功能对操作系统的安全性有着十分重要的作用。



下面将在Windows的本地安全策略中开启审核功能，其具体操作如下。



第1步：打开控制面板

在系统桌面上选择“开始”/“控制面板”命令，打开“控制面板”窗口。



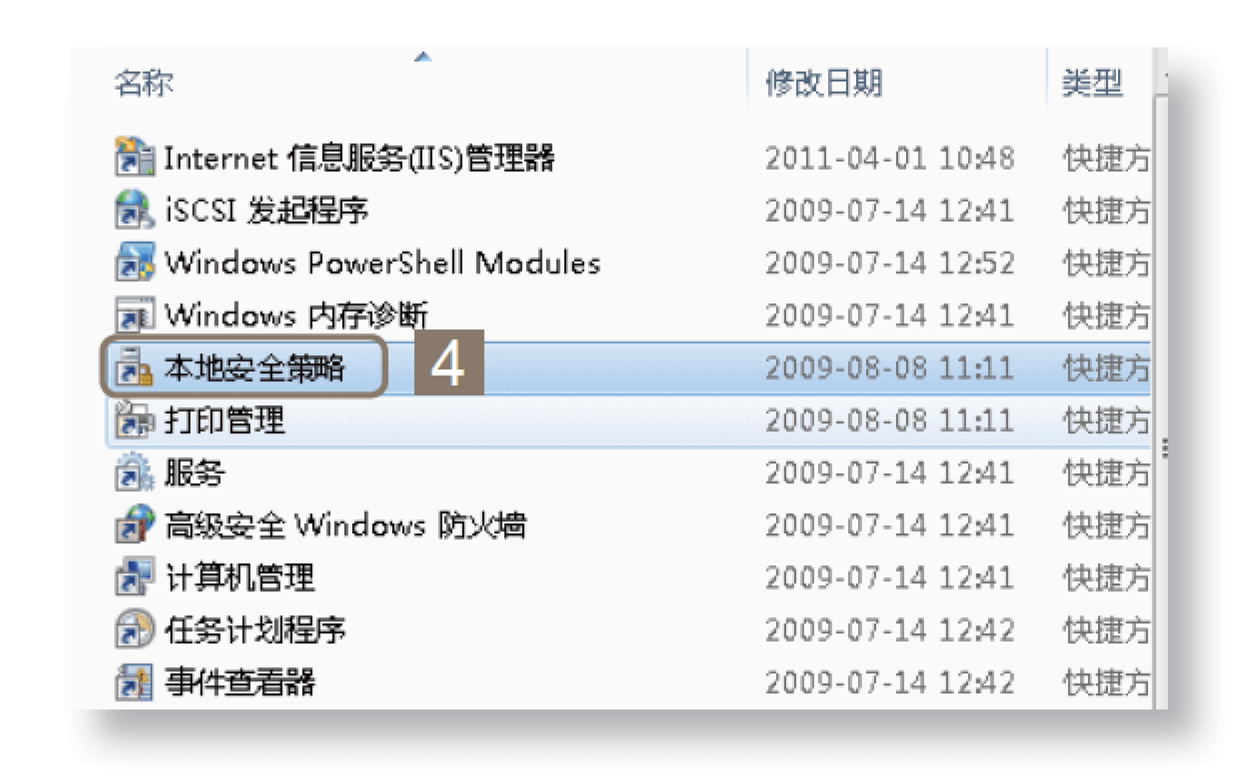
第2步：打开“管理工具”窗口

在控制面板右上角的“查看方式”下拉列表框中选择“大图标”选项，待图标转换完成后，在其中单击“管理工具”超链接，打开“管理工具”窗口。

教你一招

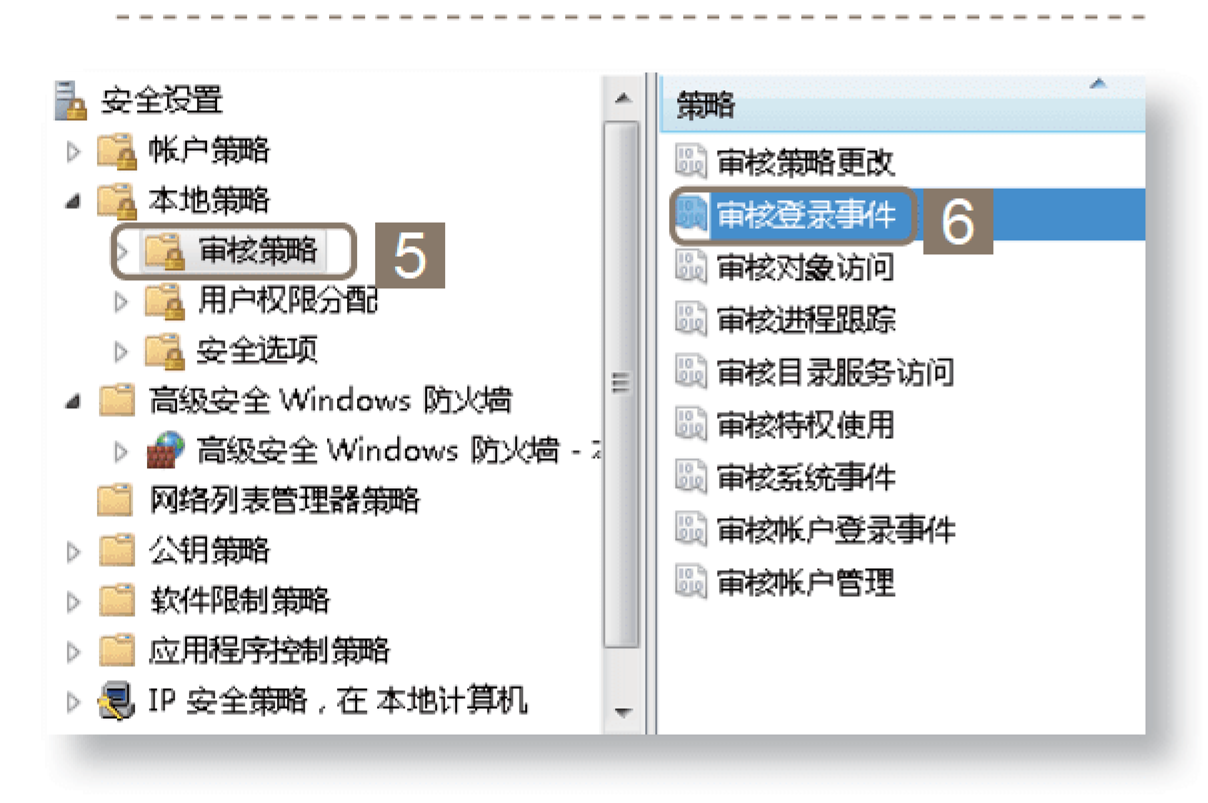
设置“分类查看”控制面板设置

在控制面板的“查看方式”下拉列表框中选择“类别”选项，在其下的窗口中将列出主要功能的列表项。



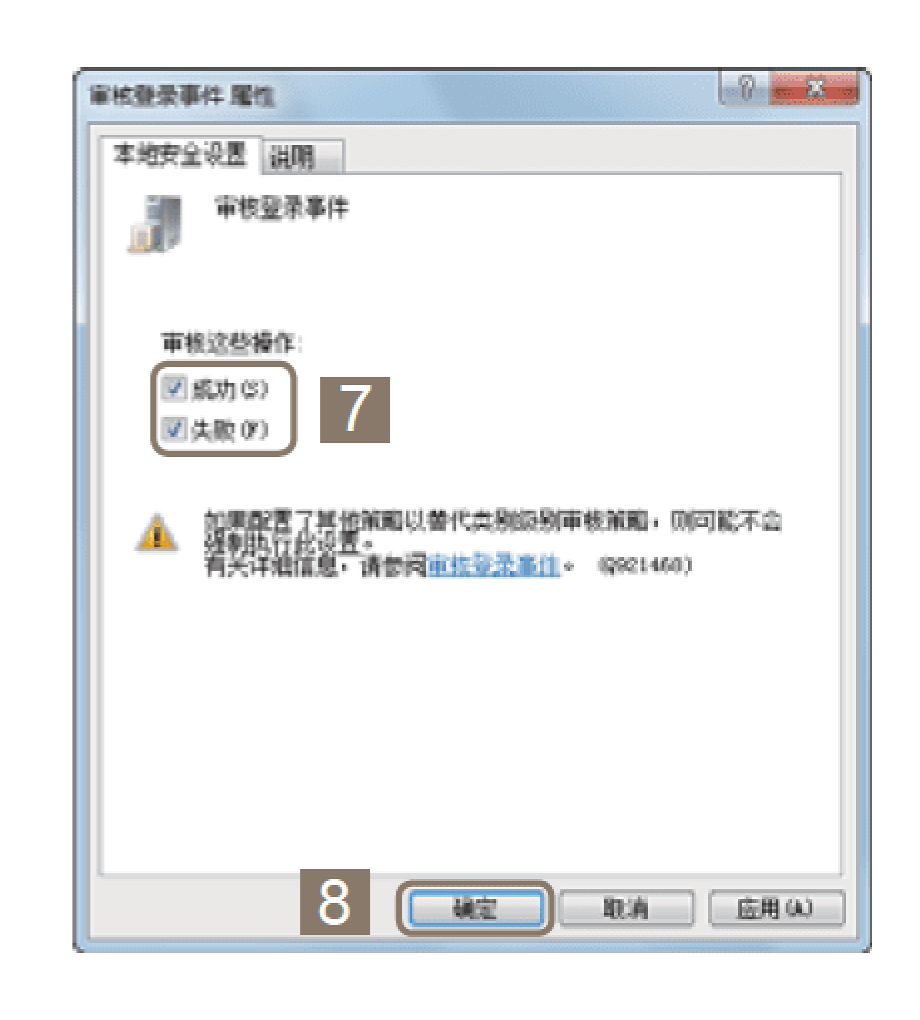
第3步：打开“本地安全策略”窗口

在打开的窗口中双击“本地安全策略”选项，打开“本地安全策略”窗口。



第4步：打开“审核登录事件 属性”对话框

在打开窗口左侧的窗格中展开“安全设置/本地策略/审核策略”选项，在其右侧窗格中双击“审核登录事件”选项，打开“审核登录事件 属性”对话框。



第5步：开启审核功能

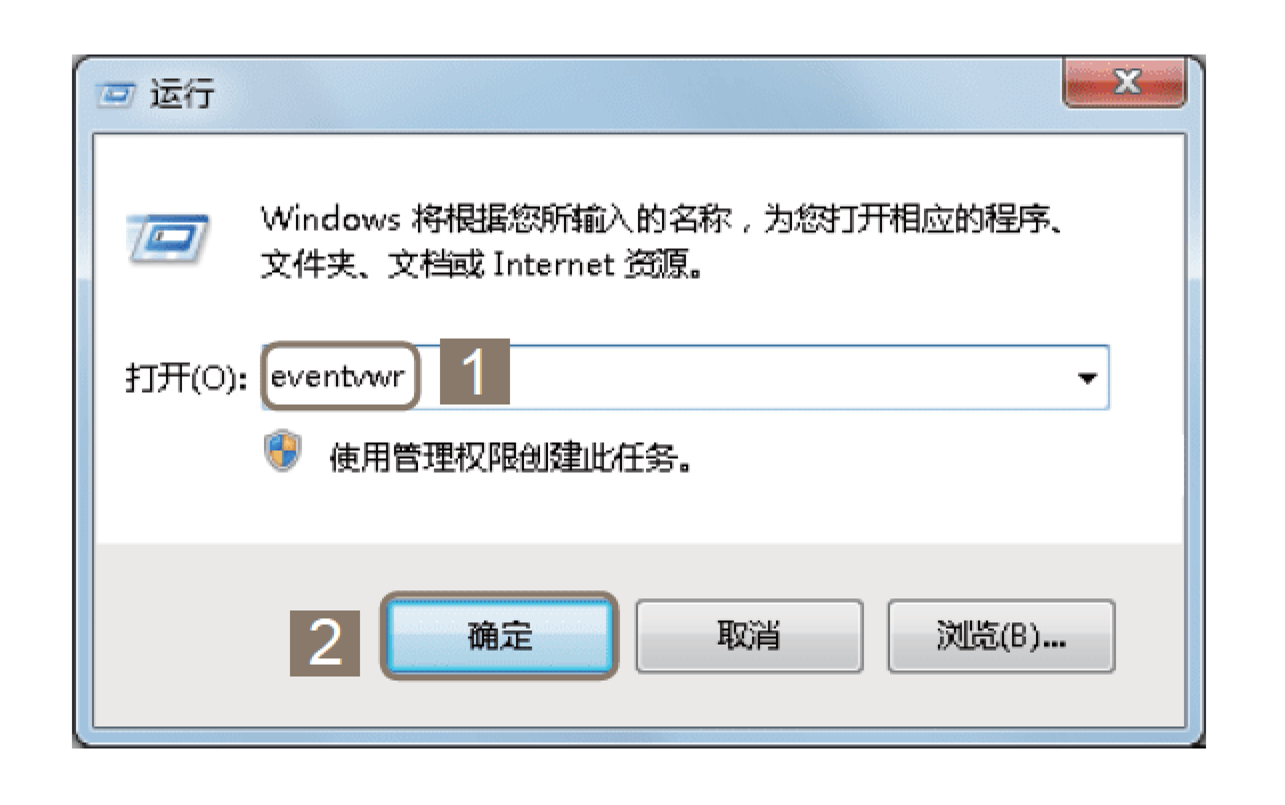
在打开的“审核登录事件 属性”对话框中选中“成功”与“失败”复选框，单击 确定 按钮即可对登录系统的操作进行审核。

5.4.2 检查日志

在Windows操作系统中，可以通过事件查看器来检查日志，该功能需与系统的审核功能结合使用才能达到审核检测的效果。系统的检查日志记录了电脑发生错误的时间和原因，用户可根据记录的信息对电脑进行相应的设置。



下面将打开事件查看器查看操作系统的审核日志，并对其进行操作，其具体操作如下。



第1步：打开事件查看器

选择“开始”/“运行”命令，打开“运行”对话框，在其中的“打开”下拉列表框中输入“eventvwr”，然后单击【确定】按钮，即可打开“事件查看器”窗口。



第2步：查看日志

在打开窗口的左侧窗格中展开“事件查看器/Windows日志/应用程序”选项，在其右侧窗格中可查看到Windows的错误日志。

提示：在其左侧窗格中还可选择“安全”、Setup、“系统”和“转发事件”等选项查看其日志信息。



第3步：打开日志属性对话框

在日志列表中选择一项错误日志选项，然后在其右侧窗格中单击“属性”超链接，打开该日志的属性对话框。

第4步：设置日志显示并清除

在打开的对话框中可查看该日志的详细信息，在“达到事件日志最大大小时”栏中选中“按需要覆盖事件（旧事件优先）”单选按钮，然后单击【清除日志(R)】按钮清除日志，单击【确定】按钮保存设置。



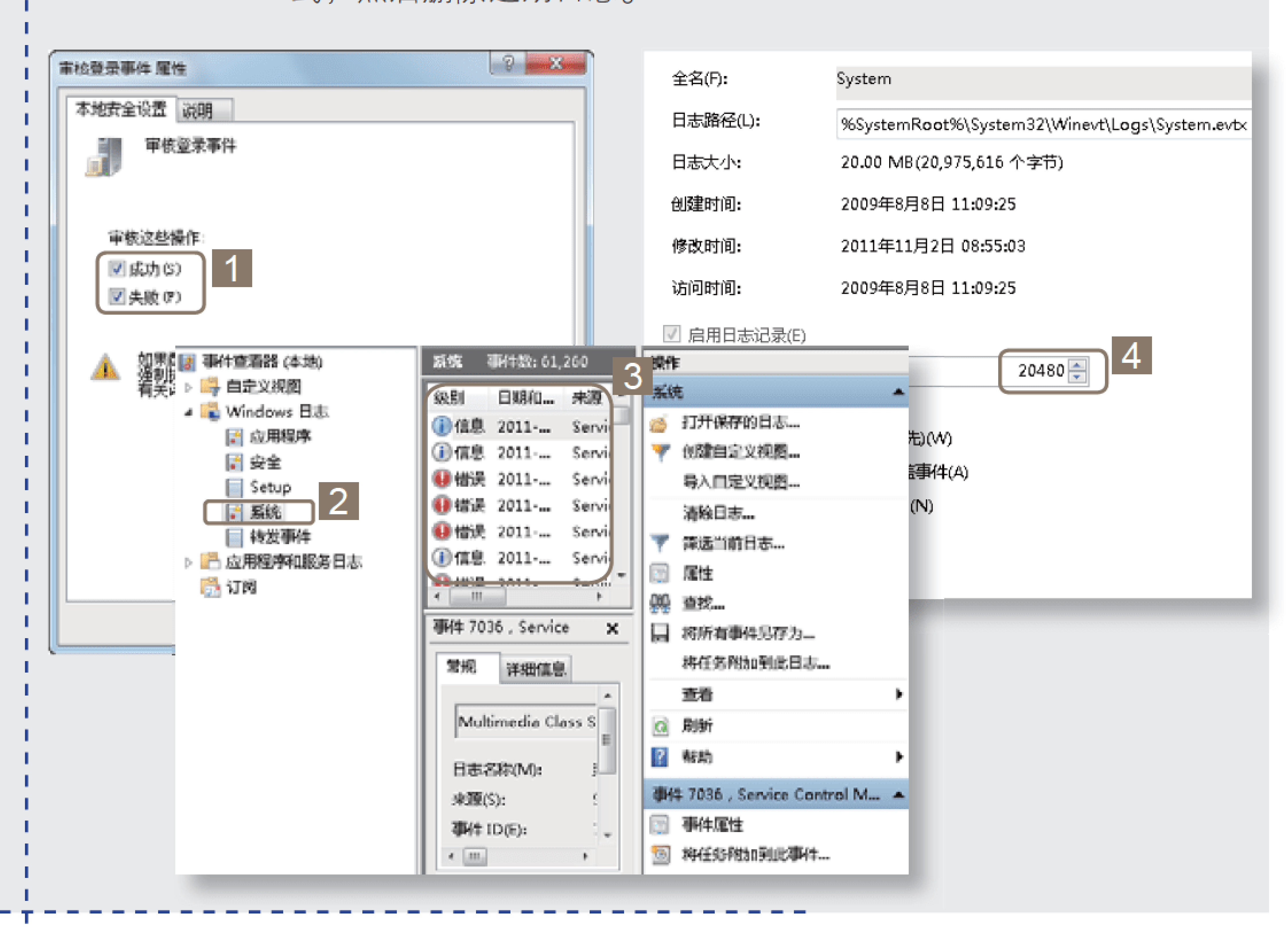
跟我练习

为了及时发现操作系统的问题，娜娜将开启系统的审核功能，并定期审核日志进行查看

任务1：打开“本地安全策略”窗口，在其中的“审核策略”选项中启用“审核登录事件”功能。

任务2：开启审核功能后，娜娜将定期打开“事件查看器”窗口对操作系统的错误日志进行查看并及时作出处理。

任务3：设置操作系统的日志最大容量及达到最大容量时日志的处理方式，然后删除近期日志。

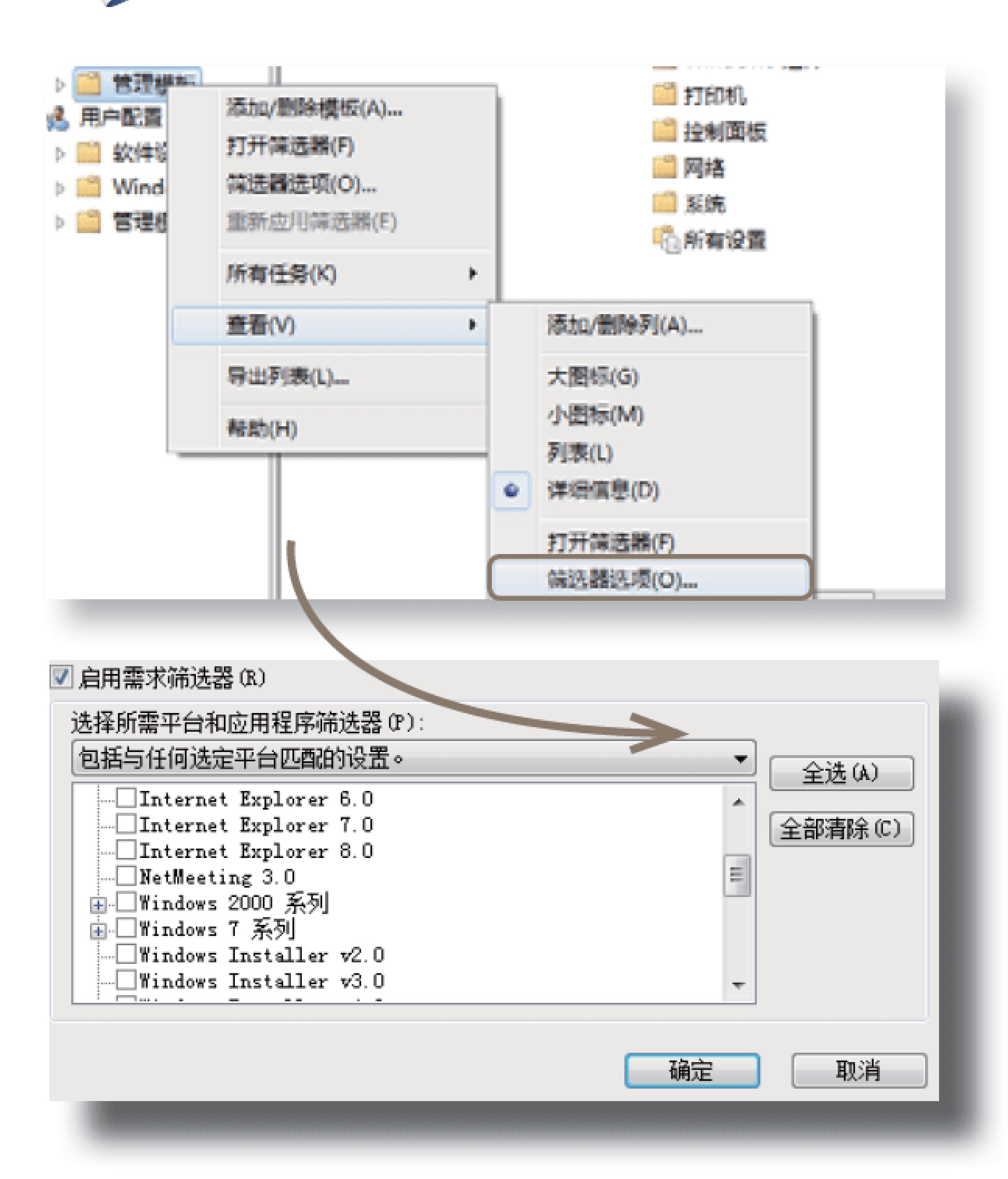


5.5 更进一步——使用组策略和注册表小秘招

通过前面的学习，娜娜不仅了解了什么是漏洞、组策略和注册表，而且还学会了怎样进行修复漏洞和利用组策略和注册表来限制用户使用电脑的相关权限。阿伟确定娜娜已经掌握了他教的知识后，决定再教娜娜几个小技巧。



第1招 暂时隐藏不用的策略



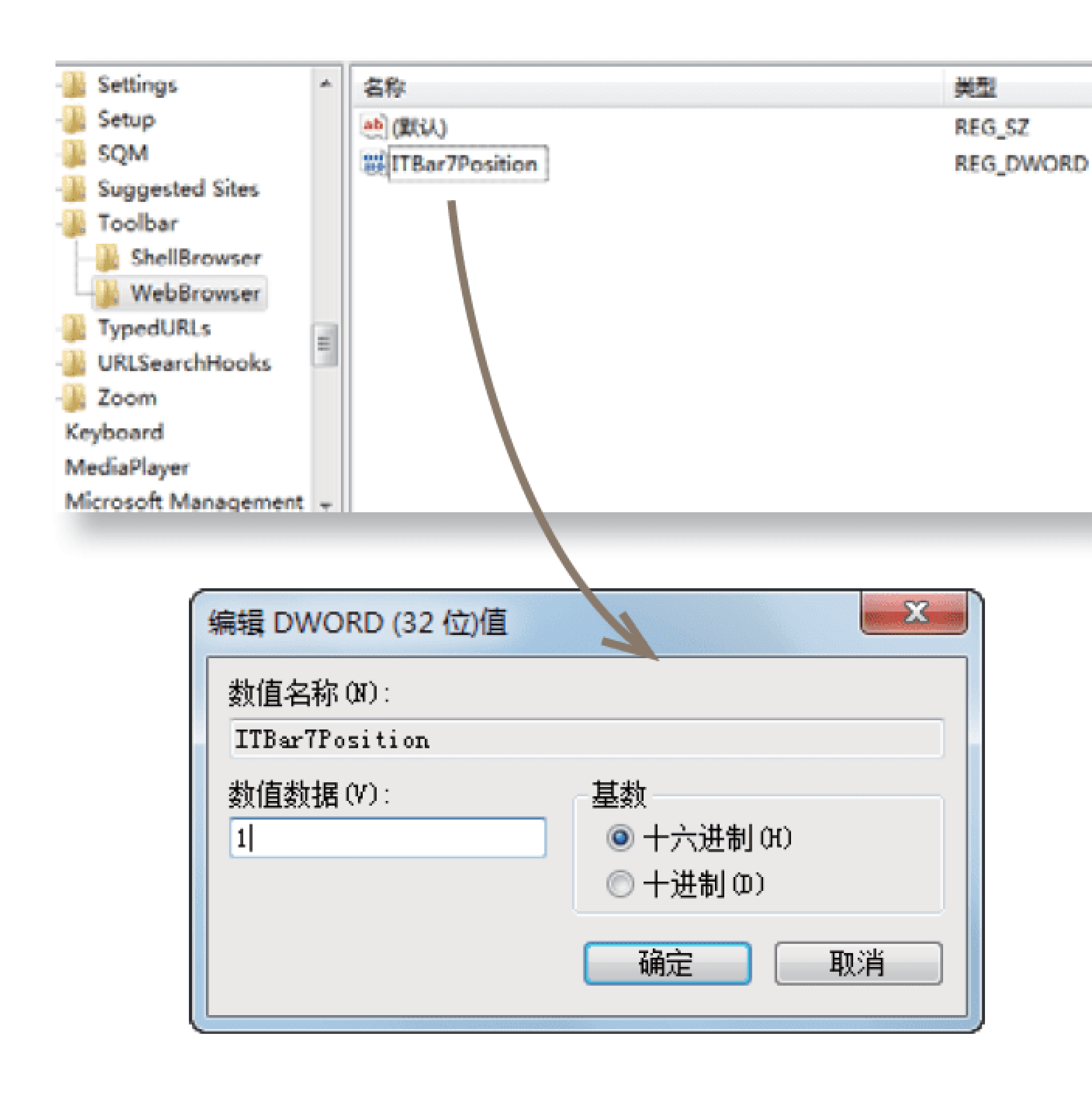
为了避免被组策略编辑器里名目繁多的策略弄得头晕眼花，这时候就可以使用组策略编辑器的“筛选”功能暂时隐藏不用的策略。

①打开组策略编辑器，在其左侧窗格中选择要隐藏策略的目录。

②单击鼠标右键，在弹出的快捷菜单中选择“查看”/“筛选器选项”命令，打开相应的对话框。

③在打开的对话框中选中“启用需求筛选器”复选框，在其下拉列表中选择筛选的条件，然后单击 确定 按钮。

第2招 将IE菜单栏移动到上方



为了使浏览器更加方便用户查看，使其更具个性化，可以通过注册表使菜单栏移动到浏览器的最上方，其方法如下：

①打开注册表编辑器，在其左侧窗格中依次展开HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/Toolbar\WebBrowser选项。

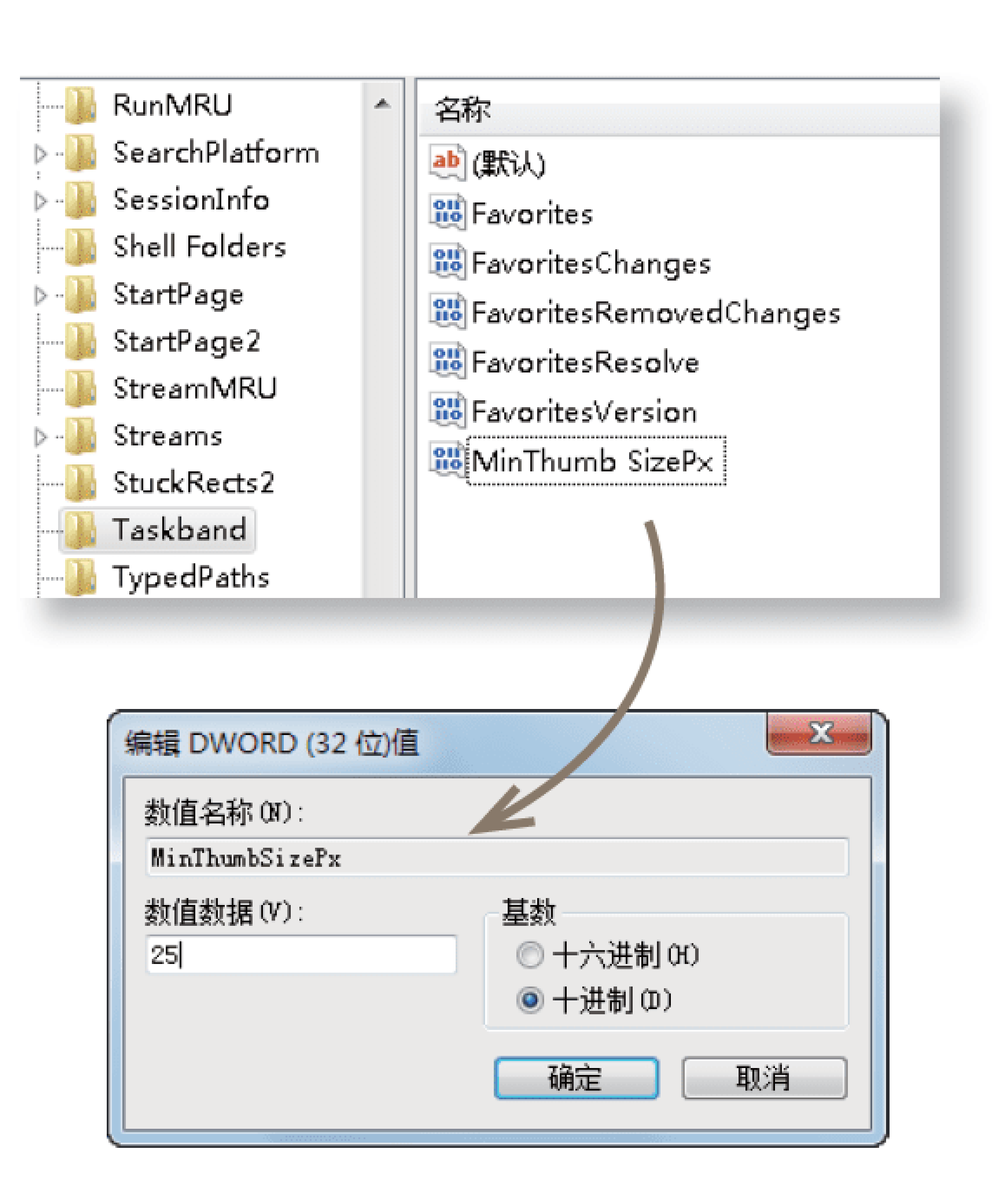
②在右侧窗格中新建一个名为ITBar7Position的DWORD值，并把数值数据设置为1（十六进制）。

第3招 调节Windows 7任务栏缩略图预览的大小

在Windows 7中，可以通过修改注册表来调节任务栏缩略图预览的大小，其方法如下：

①打开注册表编辑器，在其左侧窗格中依次展开HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Taskband选项。

②新建一个名为MinThumbSizePx的DWORD值，并把数值设置为x（十进制）。



提示：x指除了230以外的数值，因为系统默认就是230。

5.6 活学活用

（1）使用360安全卫士扫描系统中存在的漏洞，并将扫描的高危漏洞进行智能修复，以提高操作系统的安全性。

（2）浏览组策略中的相关设置选项，并在其中根据需要启用相关策略，使其更好地保护操作系统的安全。

（3）根据学过的方法将自己电脑中的注册表进行备份，并查询相关资料利用注册表对电脑中的软件设置进行优化。



☑ 想知道怎样来加固电脑的安全防御吗？

☑ 还在为经常被黑客、病毒和木马侵犯而担忧吗？

☑ 想知道怎样使用防火墙来阻止有害侵犯吗？

☑ 还在为电脑中应用程序的出错而不知所措吗？



第 06 章 打造安全堡垒——防火墙

今天，阿伟打算给娜娜讲解一些关于防火墙方面的知识。为了让娜娜了解防火墙的作用，阿伟首先在电脑上进行演示，边演示边讲解：“防火墙不仅可以限制网络中服务的使用或其他用户访问电脑，而且还可以对本地电脑中的应用程序进行控制……”看着阿伟的演示，娜娜被这种功能吸引住了，她催促阿伟赶紧告诉她怎么使用这新鲜的功能。

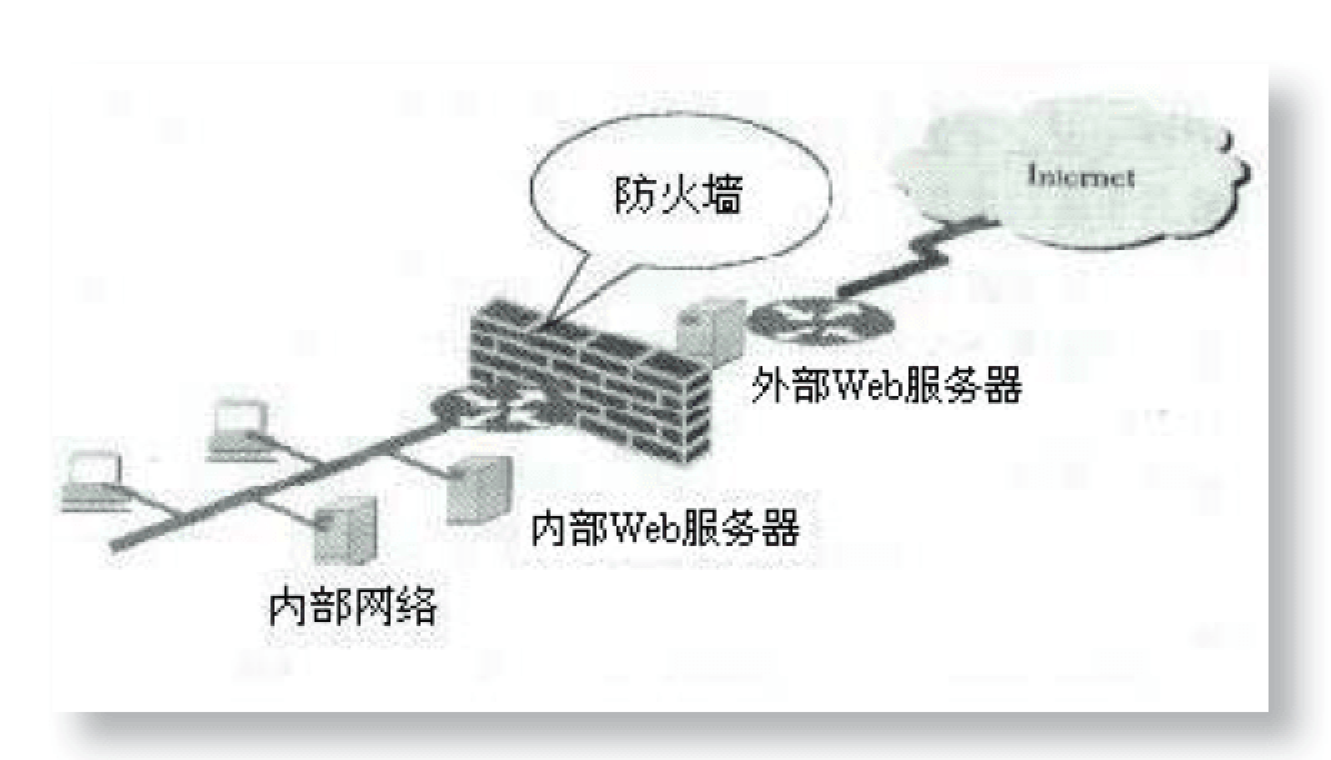
6.1 认识防火墙

阿伟告诉娜娜："虽然你知道了防火墙的这些功能，但这只是它很小的一部分，防火墙的功能很强大，要完全掌握它还需要认真学习。"娜娜听了心想，既然防火墙的功能这么多，还是应该从最基础的开始学习，避免学习完了连防火墙到底是什么都还弄不清楚。于是，她就让阿伟首先给她讲解防火墙的基本知识。

6.1.1 什么是防火墙

防火墙可为电脑筑起一道"坚固的防线"，在抵御外界攻击、杜绝病毒入侵等安全方面有着不可替代的作用。

网络中的防火墙是一种将内部网和Internet分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许"同意"的数据进入网络，同时将"不同意"的数据拒之门外，最大限度地防止网络中的黑客访问网络。换句话说，已安装防火墙而不通过防火墙，内部网就无法访问Internet，Internet中的其他用户也无法和内部网进行通信。



提示：防火墙就是一个位于电脑和它所连接的网络之间的软件。该电脑流入流出的所有网络通信均要经过防火墙。

6.1.2 防火墙的功能

防火墙可对经过它的网络通信进行扫描，从而过滤掉一些攻击，还可以关闭和禁止特定端口的流出通信，封锁木马的入侵渠道。除此之外，它还可以禁止来自特殊站点的访问，以防止来自不明入侵者的所有通信。



下面将对防火墙的功能进行简单的介绍。



- **防火墙是网络安全的屏障：** 防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过过滤的应用协议才能通过防火墙，所以使网络环境变得更安全。
- **强化网络安全策略：** 通过防火墙的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）进行配置。与将网络安全问题分散到各个主机上相比，防火墙的安全管理更集中且经济。
- **对网络存取和访问进行监控审计：** 防火墙能记录所有经过它的访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。
- **防止内部信息的外泄：** 通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。

6.1.3 个人电脑中使用的防火墙

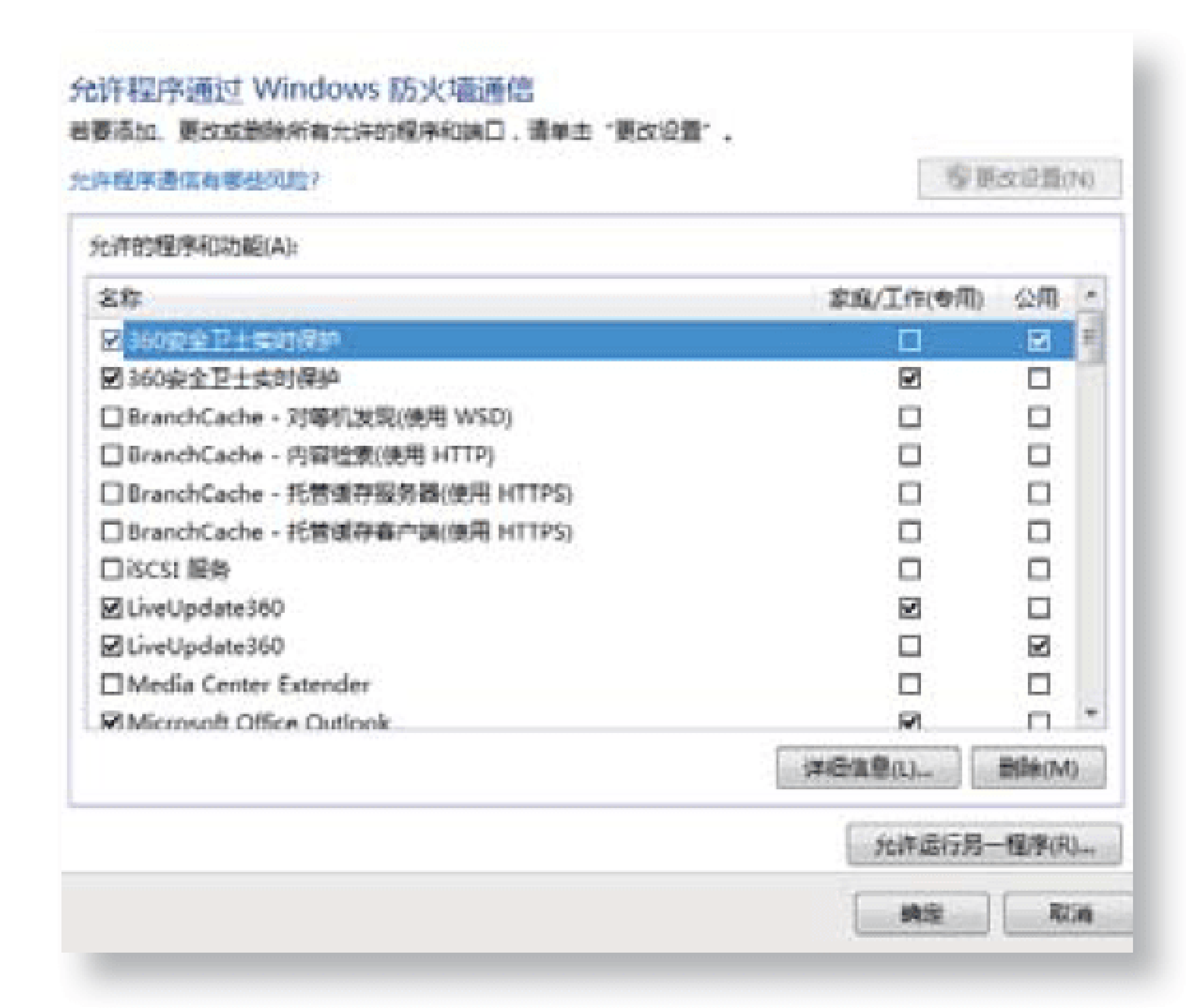
个人电脑中的防火墙可分为Windows自带的防火墙和网络防火墙两种。系统自带的防火墙具有简单的操作界面，并且设置完成后发现有错误可恢复默认设置。网络防火墙是一个位于电脑和连接网络之间的软件，流入流出电脑的所有网络通信均要经过此防火墙。

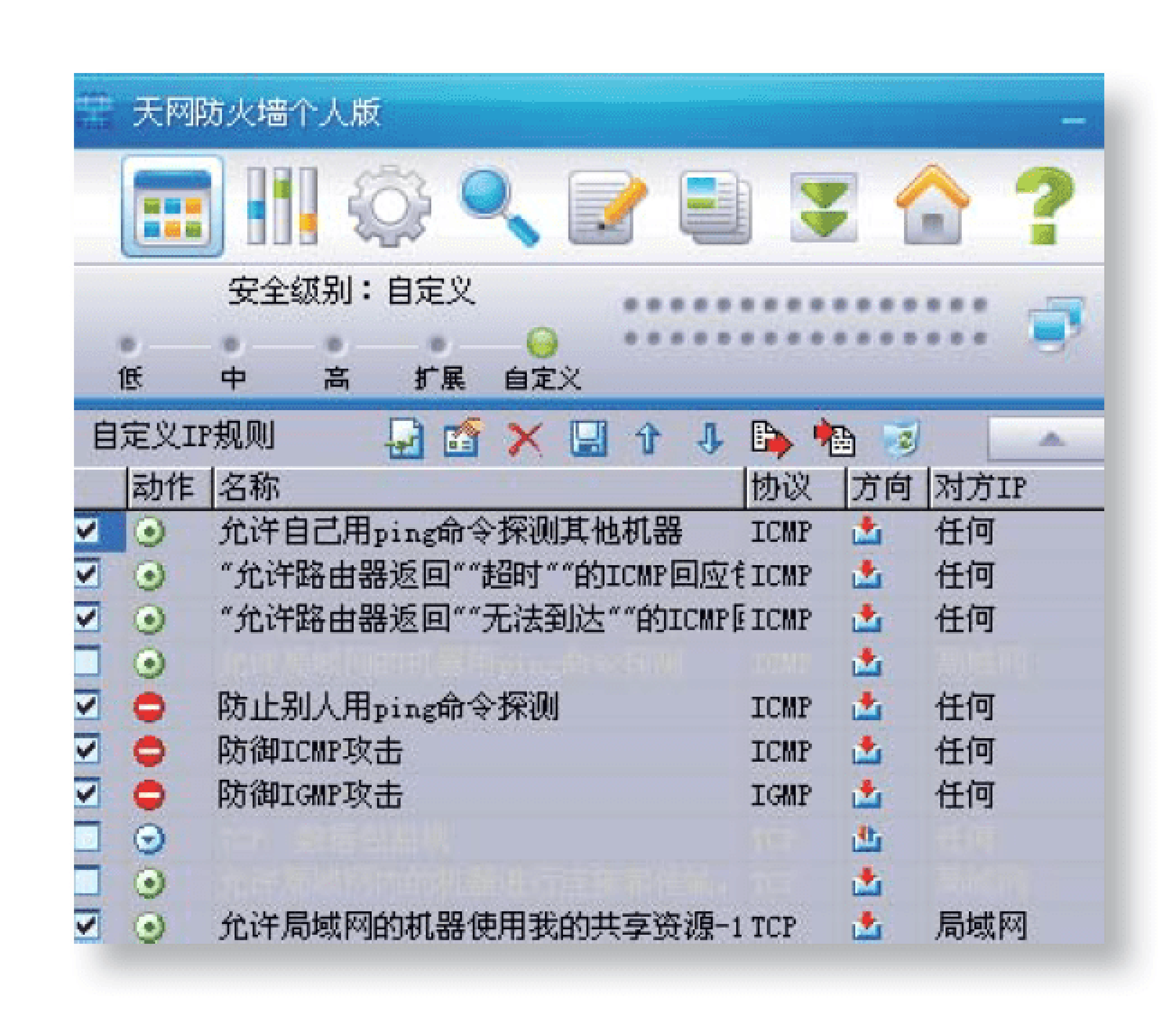


下面将对Windows自带防火墙和网络防火墙进行简单介绍。

1. Windows自带防火墙

Windows XP中的防火墙软件仅提供简单和基本的功能，且只能保护入站流量，阻止任何非本机启动的入站连接。Windows Vista的防火墙是建立在新的Windows过滤平台上的，该防火墙添加了通过高级安全MMC管理单元过滤出站流量的功能。Windows 7中的防火墙可以通过控制面板访问高级设置，而不需要创建空的MMC并添加一个管理单元。





2. 天网防火墙

天网防火墙个人版是个人电脑中使用较为广泛的网络防火墙，它能根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和互联网，可针对来自不同网络的信息设置不同的安全方案，适合于任何方式上网的用户。

3. 瑞星防火墙

瑞星防火墙具有拦截网络攻击和阻止黑客攻击系统等功能，还能最大程度地解决“肉鸡”和“网络僵尸”对网络造成的安全威胁；其恶意网址拦截功能能够保护用户在访问网页时不被病毒及钓鱼网页侵害。瑞星防火墙具有完备的规则设置，能有效地监控任何网络连接，从而保护网络不受黑客的攻击。



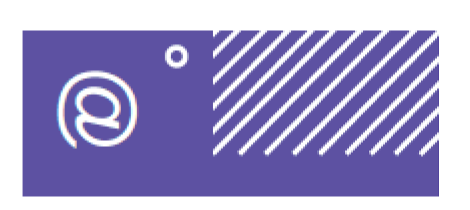
6.1.4 防火墙的工作原理

所谓防火墙，指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，它是一种获取安全性方法的形象说法。

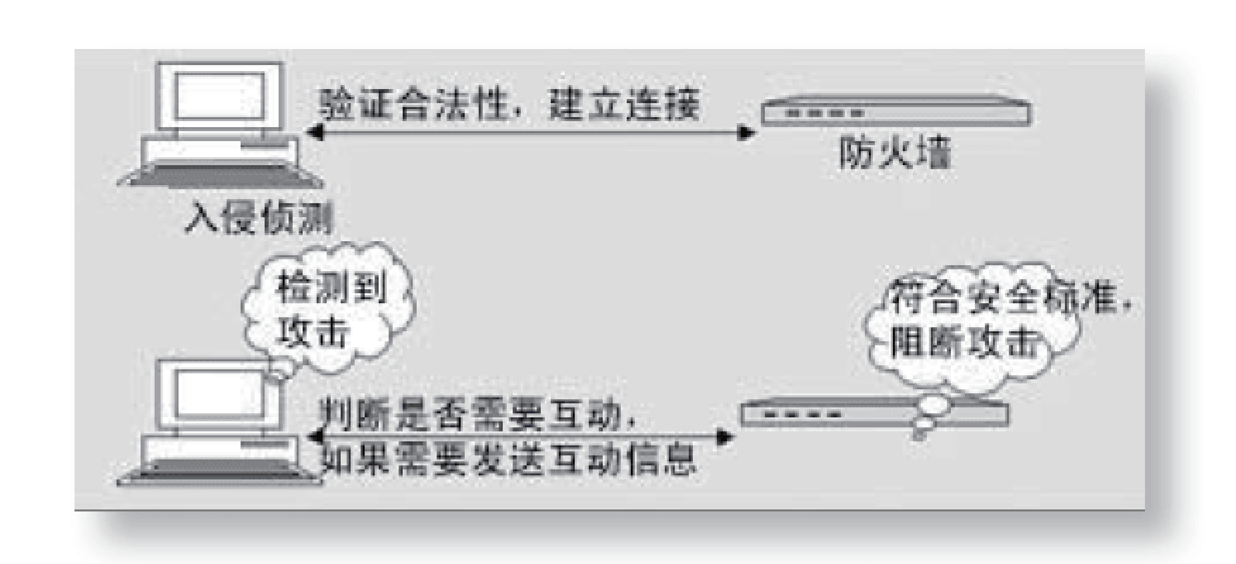
新手解惑

Q：防火墙主要由哪几部分组成？其作用是什么？

A：防火墙主要由过滤器和入侵检测组成。过滤器通过检查单个包的地址、协议和端口等信息来决定是否允许此数据包通过。入侵检测提供了全面的网络保护功能，其内置的主动防御功能可以防止破坏事件的发生。



防火墙是一种硬件和软件的结合，使Internet与Intranet之间建立起一个安全网关，从而保护内部网免受非法用户的侵入。电脑流入流出的所有网络通信均要经过此防火墙，当通信流入电脑时，将检测此通信是否符合安全标准（如检测到存在攻击行为，则阻断攻击）。



6.2 Windows自带防火墙

了解了防火墙的基本知识后，阿伟决定为娜娜讲解Windows自带防火墙的使用。他告诉娜娜："Windows自带的防火墙使用非常简单，但对于你这种刚接触防火墙的用户来说却是非常重要的，它能很好地防御攻击和保护网络安全。"娜娜听了，已经迫不及待了，让阿伟赶快开始讲解。

6.2.1 启动系统自带的防火墙

为了更好地进行网络安全管理，Windows 系统提供了防火墙功能。如果我们巧妙地使用该功能，就可以根据实际需要允许或拒绝网络信息通过，从而达到防范攻击、保护网络安全的目的。



下面将对启动系统自带防火墙的方法进行讲解，其具体操作如下。



第1步：进入防火墙设置窗口

选择"开始"/"控制面板"命令，在打开的窗口中单击"系统和安全"超链接，然后在打开的窗口中单击"Windows 防火墙"超链接。



第2步：打开自定义设置窗口

在打开窗口的左侧窗格中单击“打开或关闭Windows 防火墙”超链接，打开“自定义每种类型的网络的设置”窗口。

第3步：启动防火墙

在打开的窗口中分别选中“启用Windows 防火墙”单选按钮，然后单击确定按钮启动Windows 防火墙，防火墙将阻止新程序的运行并向用户发出提示通知。

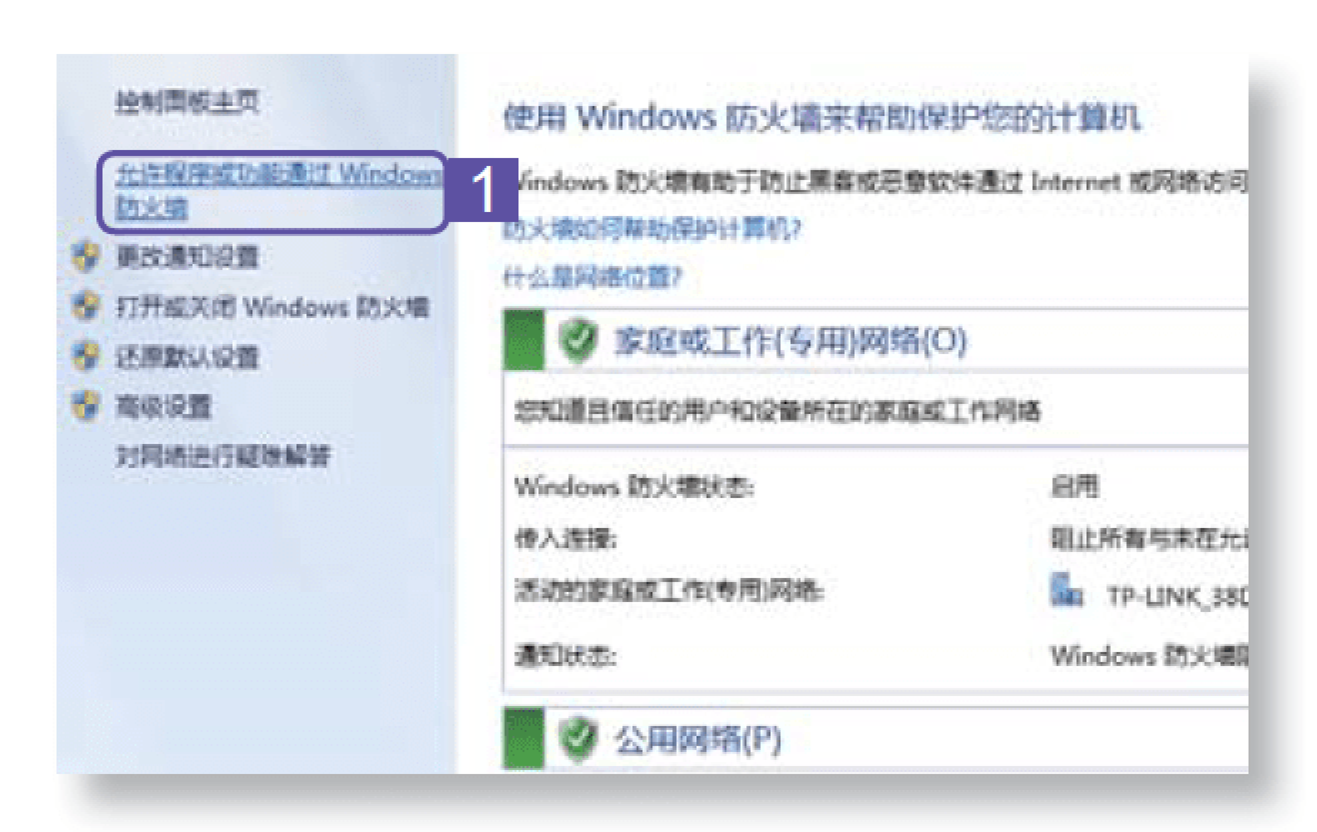


6.2.2　设置允许的程序和功能

在防火墙的允许程序设置中，可以将所要用到的程序都添加到允许通过防火墙进行通信的程序列表中，赋予它们允许进行通信的权限，这样可保证在启用防火墙的情况下仍能正常使用那些经常用到的程序和功能。



下面将对设置允许通过程序和功能的方法进行讲解，其具体操作如下。



第1步：进入允许程序设置窗口

打开“Windows 防火墙”窗口，在其左侧窗格中单击“允许程序或功能通过Windows防火墙”超链接，打开允许程序设置窗口。



第2步：设置允许的程序

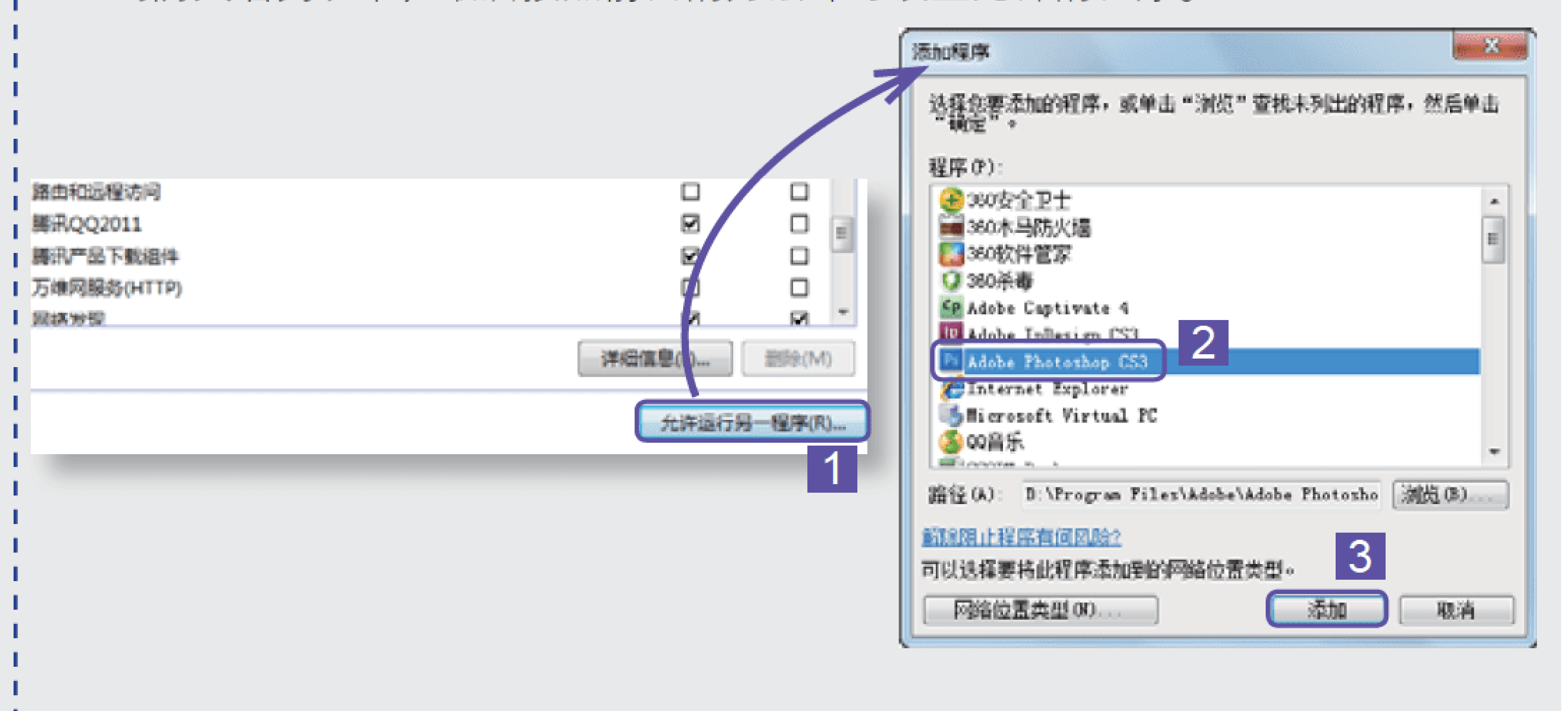
在打开窗口的“允许的程序和功能”列表框中选中需要设置允许的程序前的复选框，然后单击确定按钮完成设置。



教你一招

如何设置允许列表框中没有的程序？

如在“允许的程序和功能”列表框中没有需要设置允许的程序，可单击允许运行另一程序(R)...按钮，然后在打开对话框的“程序”列表框中选择要设置的程序或单击浏览(B)...按钮，找到要设置程序的路径，单击添加按钮将其添加到防火墙列表中，最后按照前面的方法即可设置允许的程序。



6.2.3 Windows 防火墙高级设置

在Windows防火墙高级设置中，可以详细定制规则，如设置入站规则、出站规则、连接安全规则等，并可设置端口、协议、安全连接及作用域等增强网络安全的策略。

1. 入站规则和出站规则

入站规则可为入站通信配置规则指定系统或用户、程序服务或端口和协议，并可指定应用规则的网络适配器类型。而出站规则与入站规则的作用相同，为出站通信创建或修改规则。



Q：入站规则和出站规则能做哪些操作？其作用是什么？

A：入站规则和出站规则都具有新建规则、按配置文件筛选、按状态筛选和按钮筛选等操作选项。新建规则是为了增加通信的安全性，筛选的作用则是为了方便用户查看和选择规则。



下面将讲解如何在防火墙中新建入站规则，其具体操作如下。

第1步：进入防火墙高级设置窗口

打开“Windows 防火墙”窗口，然后单击“高级设置”超链接，打开“高级安全Windows 防火墙”窗口，在其中可查看相关设置选项。





第2步：新建入站规则

在打开的窗口中单击左侧窗格中的 入站规则 按钮，即可显示入站规则的相关选项，在其右侧窗格中单击 新建规则... 按钮，打开新建向导。





第3步：设置规则类型

在打开的新建入站规则向导中可选择要创建规则的类型，通常可选择程序、端口和自定义规则，这里选中“程序”单选按钮，然后单击 下一步(N) > 按钮。



第4步：设置程序路径

在打开的向导中选中“此程序路径”单选按钮，然后单击 浏览(R)... 按钮，在打开的对话框中选择要设置规则的程序，这里设置“木马克星”程序，完成后单击 下一步(N) > 按钮。

第5步：设置允许连接

在打开的向导中选中“允许连接”单选按钮，表示在任何条件下都进行连接，然后单击 下一步(N) > 按钮。

第6步：设置规则名称并完成创建

在打开向导的“名称”文本框中输入“木马克星”，然后单击 完成(F) 按钮完成入站规则的创建。

提示：出站规则与入站规则的创建方法基本相同，这里不再赘述。

2. 连接安全规则

使用连接安全规则可以指定身份验证应用于匹配此连接安全规则的入站和出站连接的方式。有要求身份验证和请求身份验证两种，如果请求身份验证，那么即使身份验证失败也会允许连接；如果要求身份验证，则身份验证失败将丢弃连接。

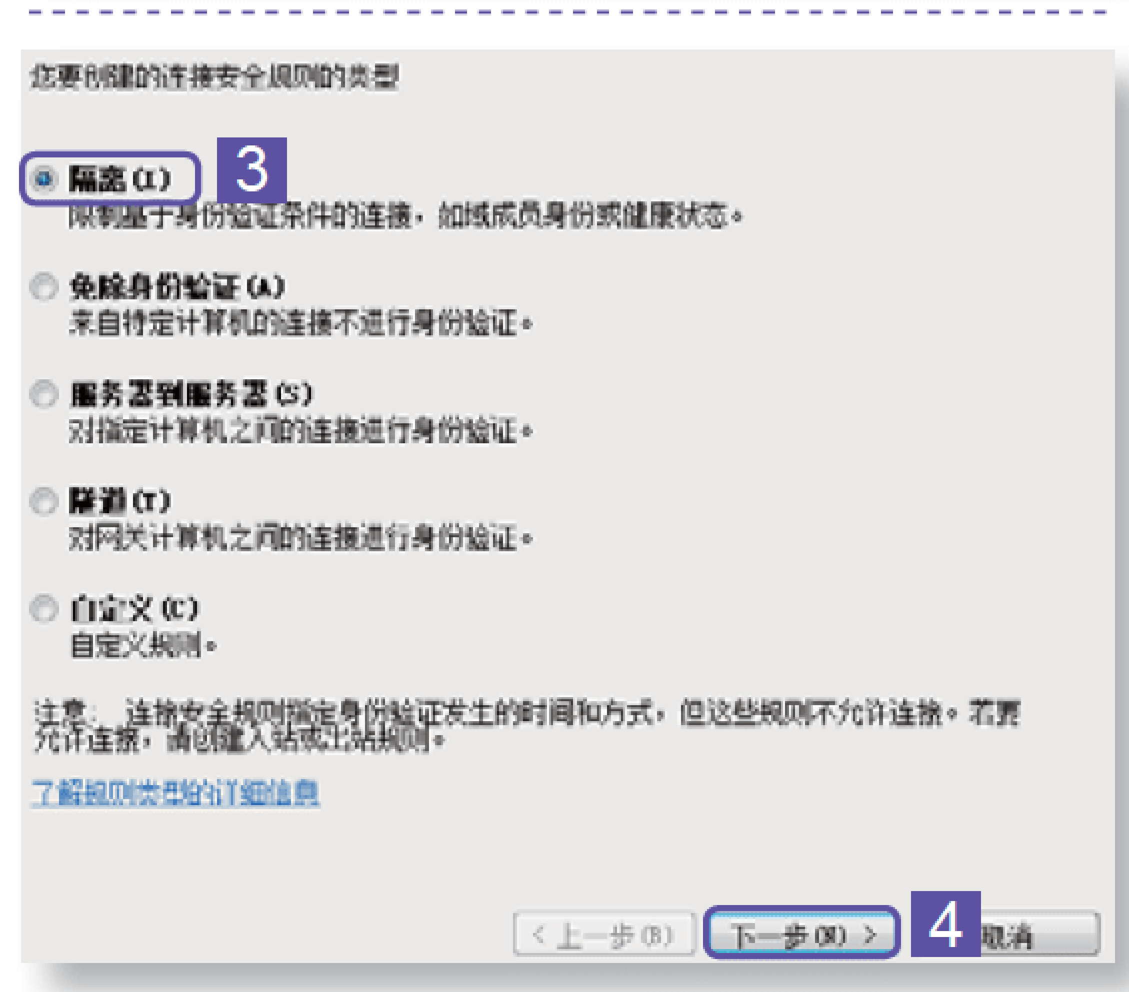


用户通过新建连接安全规则可控制连接的身份验证方式，下面将对新建安全规则进行讲解，其具体操作如下。



第1步：打开新建向导

在“高级安全Windows 防火墙”窗口中单击左侧窗格的 连接安全规则 按钮，然后在其右侧窗格中单击 新建规则... 按钮，打开新建向导。



第2步：选择规则类型

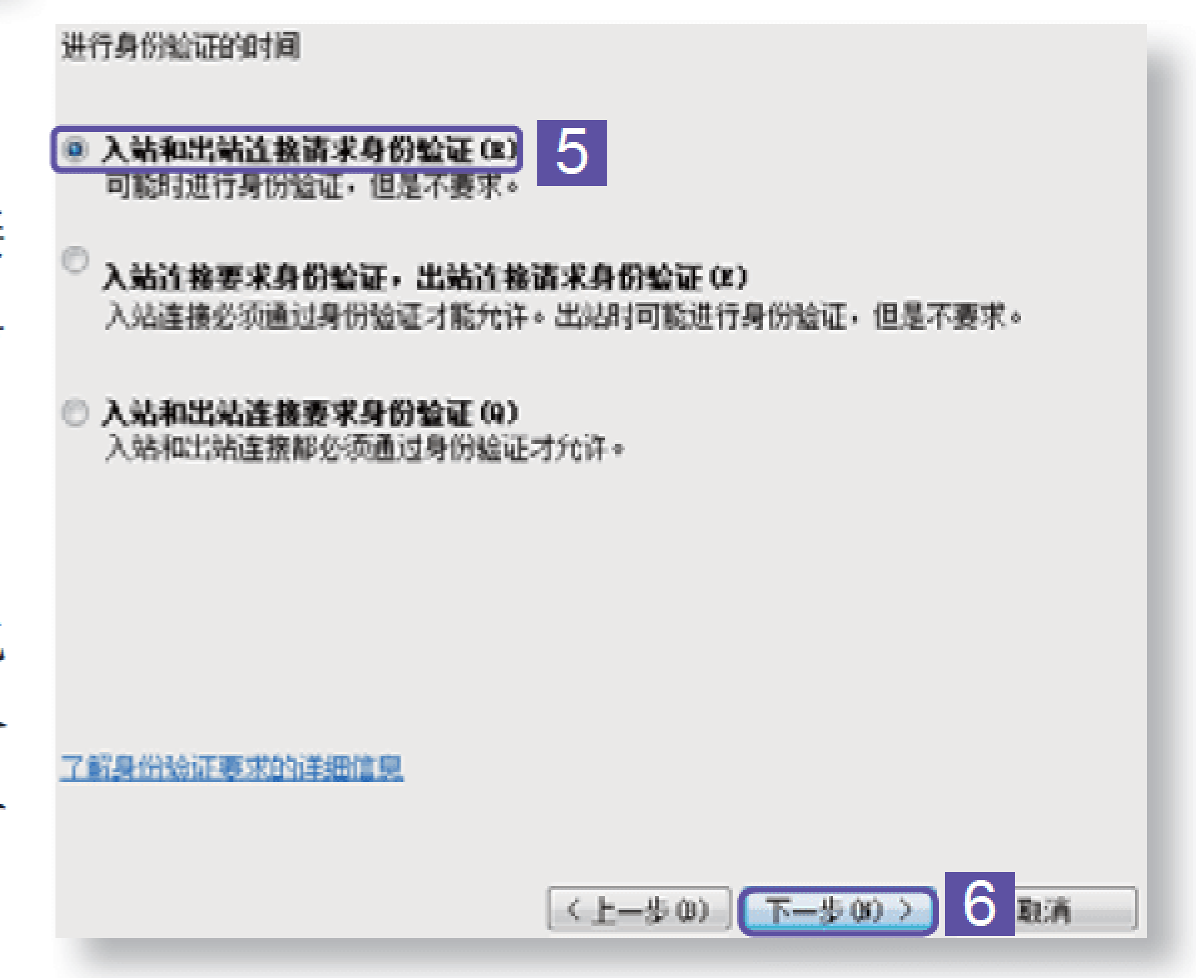
在打开的向导中选中“隔离”单选按钮，然后单击 下一步(N) > 按钮。

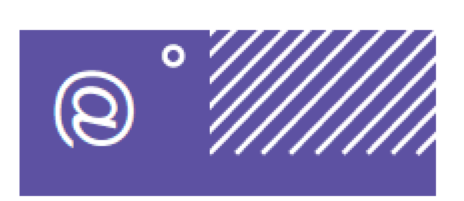
提示：“隔离”规则可根据用户定义的身份验证标准对连接进行限制。“免除身份验证”规则虽然已免除身份验证，但这些网络流量仍然可能被 Windows 防火墙阻止。

第3步：指定身份验证的要求

在打开的向导中选中“入站和出站连接请求身份验证”单选按钮，然后单击 下一步(N) > 按钮即可。

提示：该选项一般用于低安全性环境或电脑必须连接的环境，但不能执行高级安全 Windows 防火墙所具备的身份验证类型。





第4步：指定身份验证方法

在打开的向导中选中“默认值”单选按钮，然后单击 下一步(N) > 按钮。



提示：前3个选项仅在指定“隔离”或“自定义”规则类型时可用，而“高级”选项在任意类型中均可用。

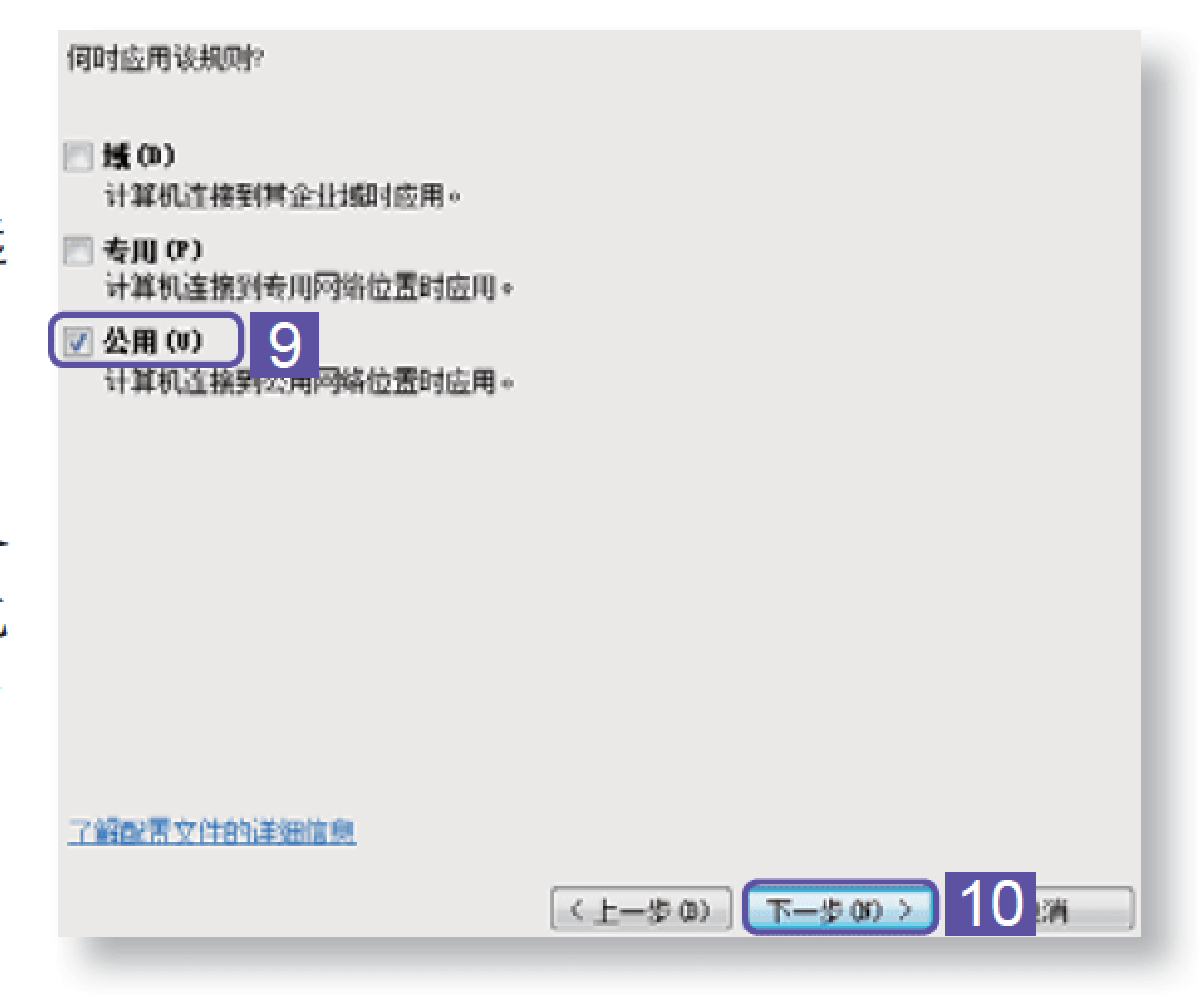
教你一招

怎样更改连接安全规则设置？

创建的连接安全规则可在“连接安全规则属性”对话框中进行更改。其方法为：双击某个规则，打开属性对话框，在“身份验证”选项卡中即可更改连接安全规则。

第5步：配置应用范围

在打开的向导中仅选中“公用”复选框，然后单击 下一步(N) > 按钮。



提示：由于电脑连接到的公用网络对安全性的控制通常不如专业网络环境严格，所以公用配置文件设置应该最为严格。

第6步：配置应用范围

在打开向导的“名称”文本框中输入“公用网连接安全规则”，然后单击 完成(F) 按钮，完成连接安全规则的创建。

教你一招

怎样更改连接安全规则设置？

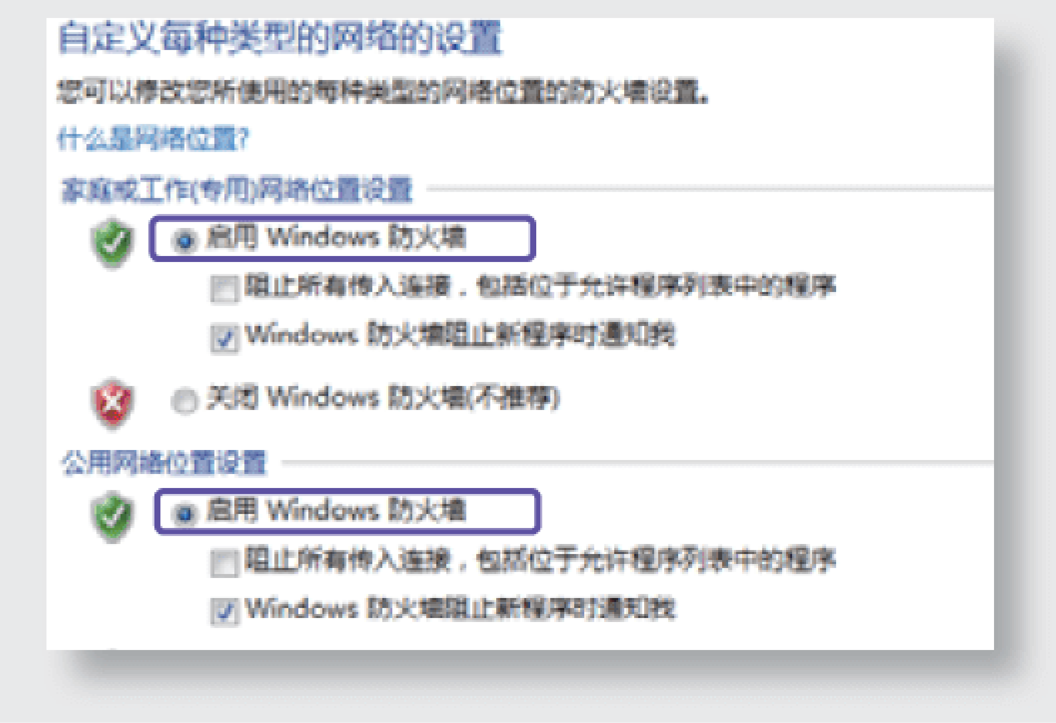
与单方面操作的防火墙规则不同，连接安全规则要求通信的双方电脑都具有采用连接安全规则的策略或其他兼容的 Internet安全策略。

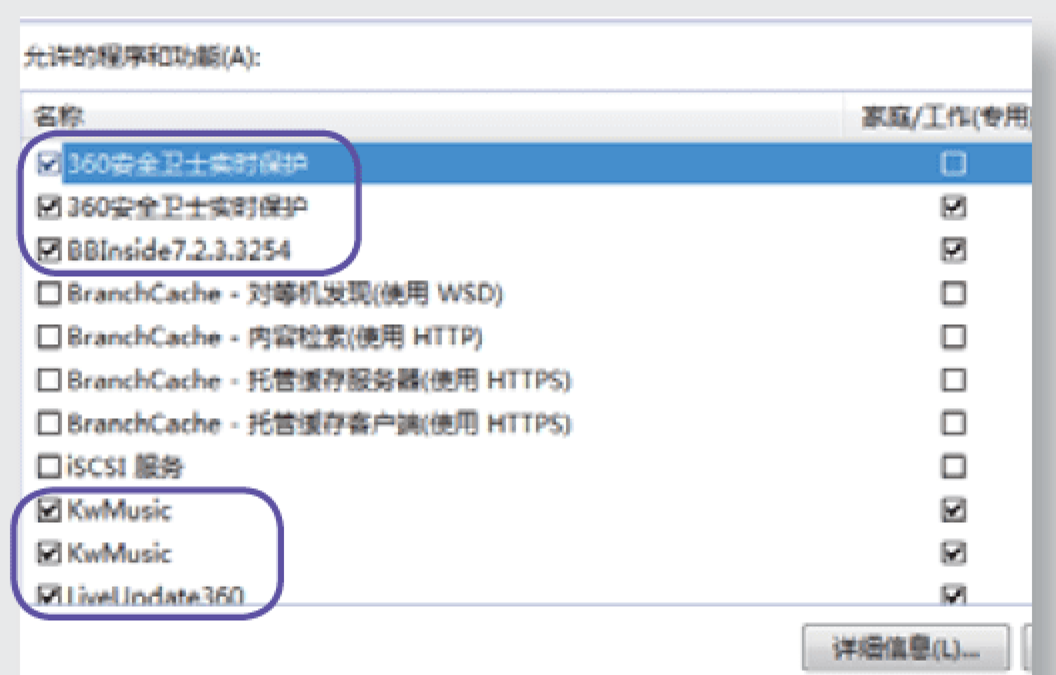
跟我练习

为了保证电脑的安全性，娜娜决定在电脑中启用Windows防火墙，并进行相关设置。

任务1：选择“开始”/“控制面板”命令，在打开的窗口中单击“Windows防火墙”超链接，打开“Windows防火墙”窗口，然后单击“打开或关闭Windows防火墙”超链接，在打开的对话框中启动防火墙。

任务2：设置允许通过防火墙的程序，并在高级设置中新建相应的入站规则和出站规则。





6.3 网络防火墙

不知不觉中，阿伟已经为娜娜讲解了Windows 防火墙的很多重要用法。娜娜在掌握了这些知识后，继续要求阿伟给她讲解网络防火墙的用法。阿伟被娜娜的积极性感染了，于是接着又为她讲解天网防火墙的使用方法。

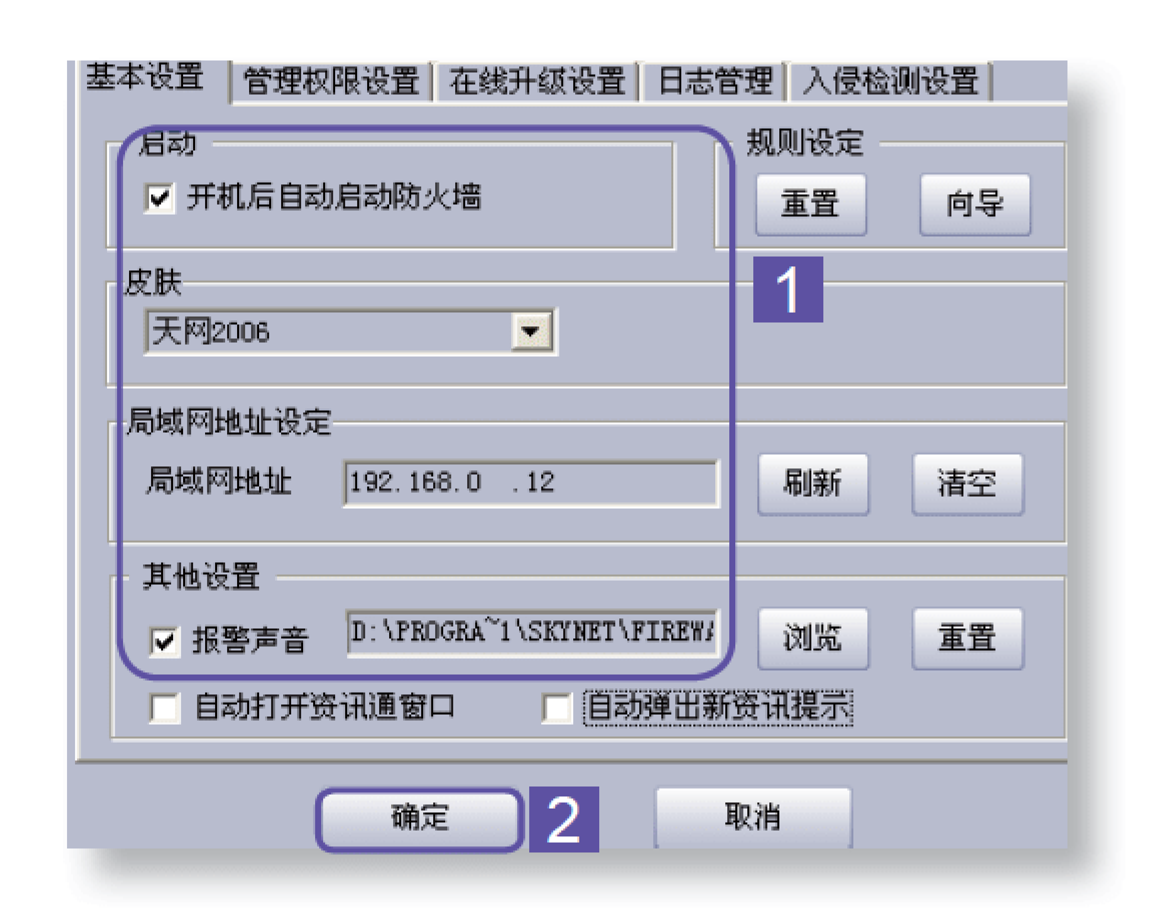
6.3.1 使用天网防火墙系统设置

使用天网防火墙前，首先应安装天网防火墙，在安装天网防火墙的过程中会要求用户进行安全级别与局域网信息等的设置，用户只需按实际情况选择即可。





下面将介绍启动天网防火墙后进行系统设置的方法，包括基本设置、管理权限设置与日志管理设置等，其具体操作如下。

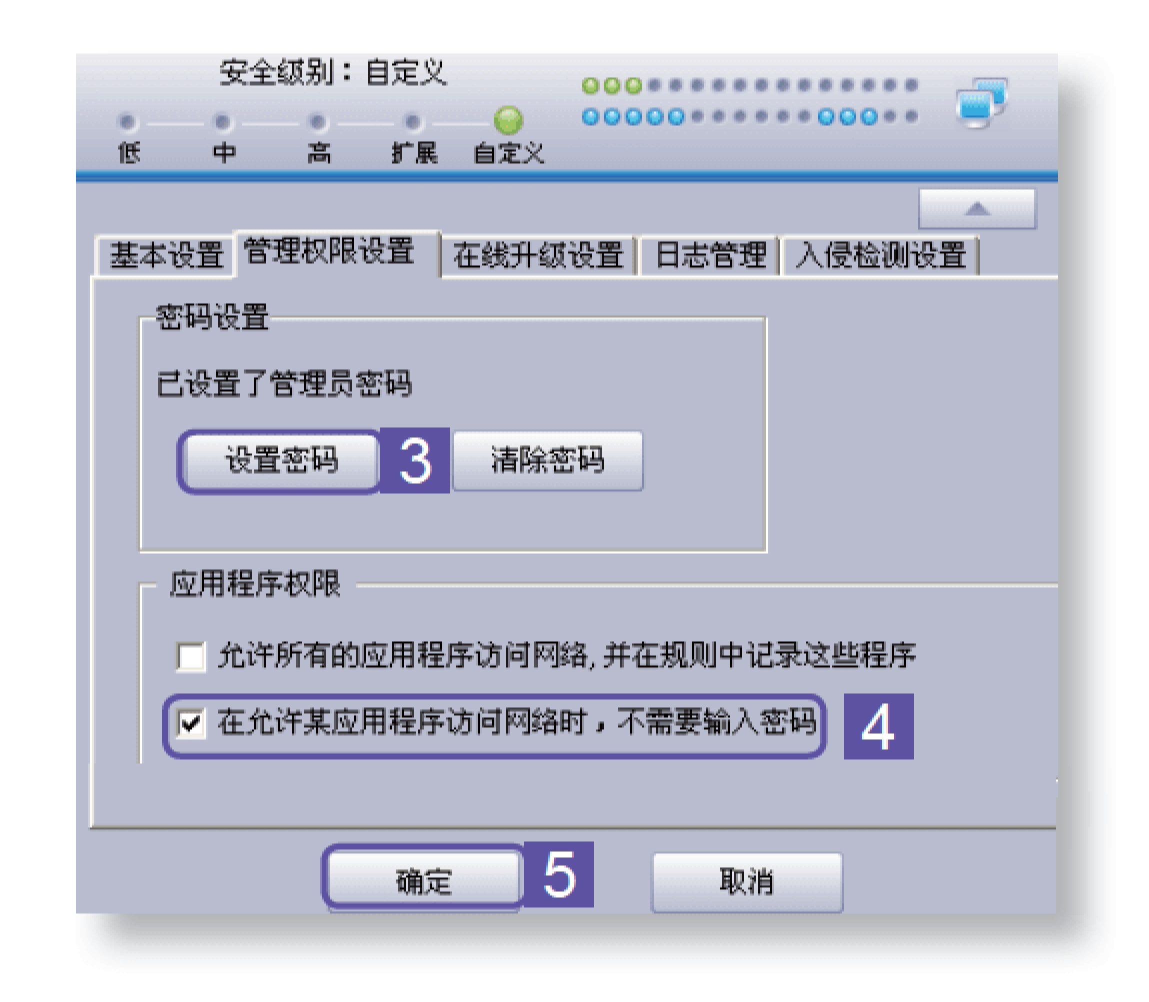


第1步：启动天网防火墙

在桌面右下角单击天网防火墙图标启动该软件，打开其工作界面，单击按钮，在打开窗口的“基本设置”选项卡中可对天网防火墙的启动、皮肤、局域网地址和报警声音等进行设置，完成后单击确定按钮。

第2步：设置管理员权限

选择“管理权限设置”选项卡，单击设置密码按钮，在打开的对话框中设置防火墙的管理员密码，选中“在允许某应用程序访问网络时，不需要输入密码”复选框，完成后单击确定按钮应用设置。



第3步：设置升级提示

选择“在线升级设置”选项卡，在“升级提示”栏中进行相应设置，这里保持默认选中“有新的升级包就提示”单选按钮，及时升级新的功能，设置完成后单击确定按钮。





第4步：设置日志管理

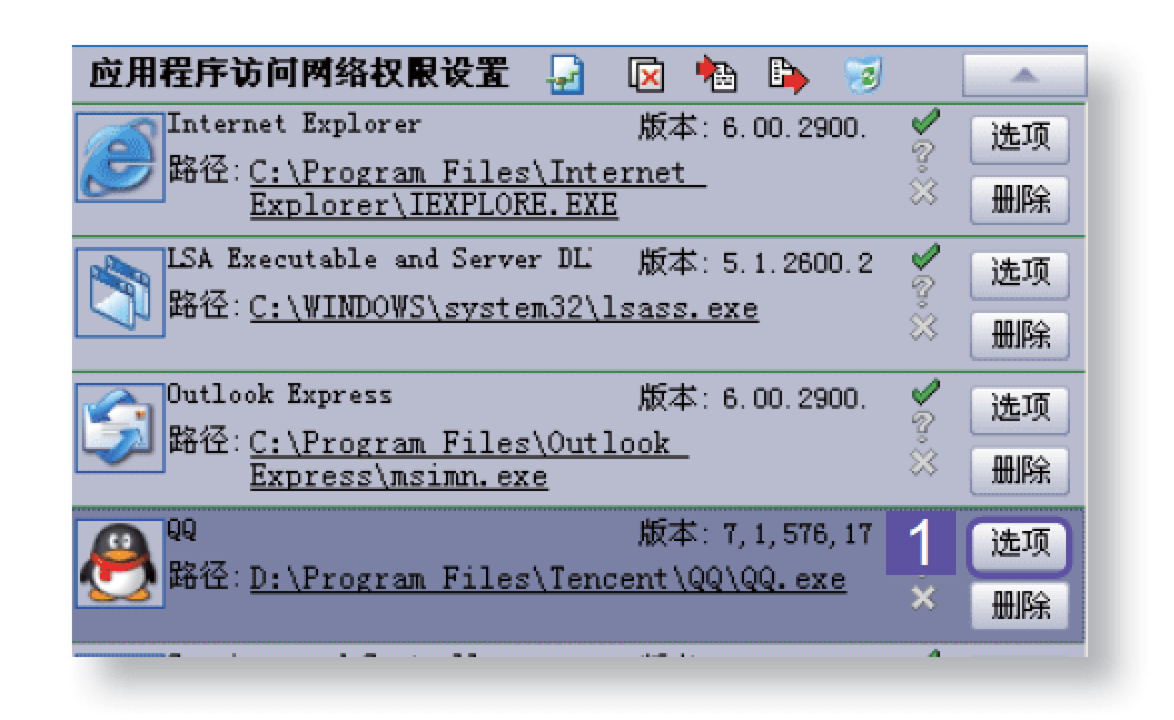
选择“日志管理”选项卡，选中“自动保存日志”复选框，单击按钮设置日志的保存位置，这里保持默认路径不变，然后单击按钮完成防火墙系统的设置。

6.3.2 设置应用程序规则

当有程序试图访问网络时，天网防火墙会打开一个提示对话框，该对话框中包含访问网络程序的相关信息。这种情况属于设置应用程序规则，在“应用程序询问网络权限设置”对话框中，用户可将常用的应用程序设置为可信任，使其能够自动访问网络。



若程序每次访问网络时都要经过防火墙的拦截，就会给用户带来很多麻烦。为避免这种情况发生，用户可将可信的、常使用的程序添加到天网防火墙的允许访问应用程序列表中。下面将以设置QQ程序的规则为例进行讲解，其具体操作如下。

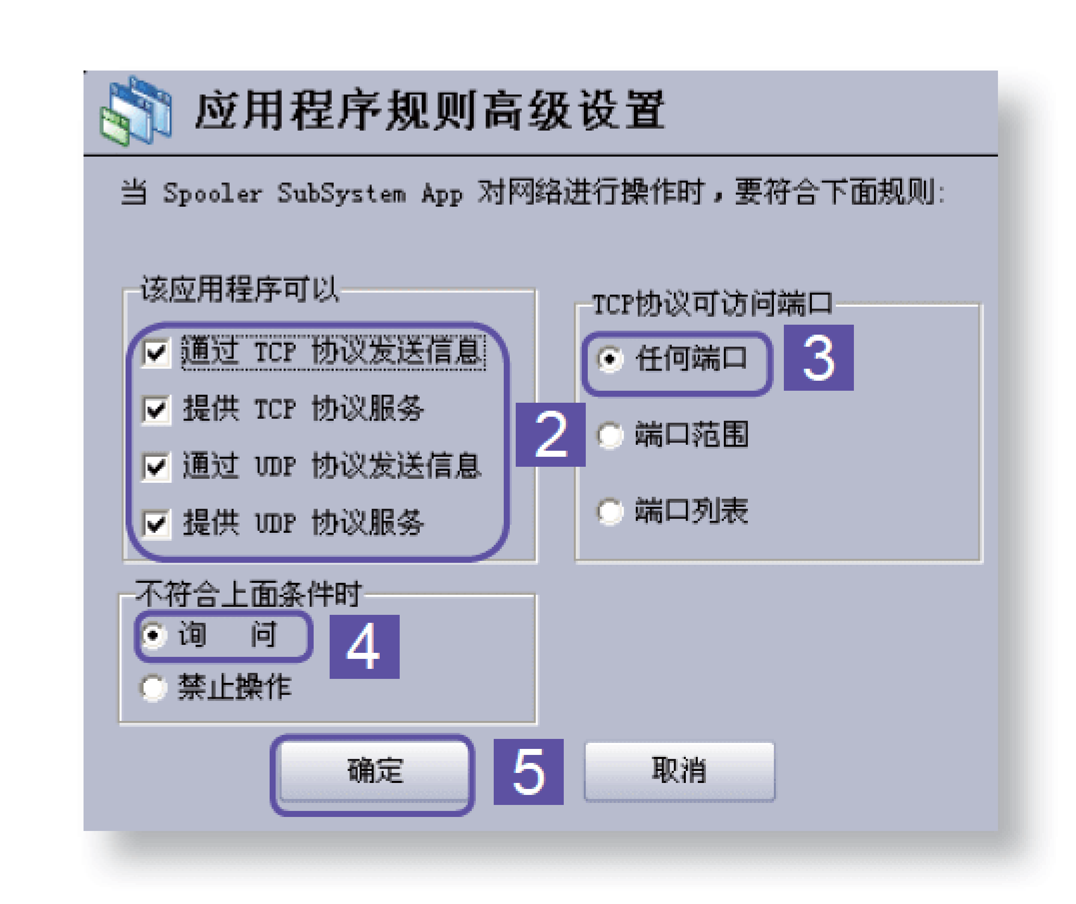


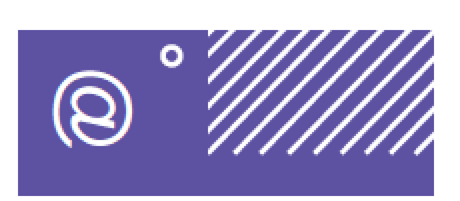
第1步：选择QQ进行设置

在天网防火墙工作界面中单击按钮，打开“应用程序访问网络权限设置”对话框，单击QQ程序栏右侧的按钮，即可对该应用程序进行规则的设置。

第2步：设置访问网络的权限

打开“应用程序规则高级设置”对话框，选中“该应用程序可以”栏中的所有复选框，选中“TCP协议可访问端口”栏中的“任何端口”单选按钮，选中“不符合上面条件时”栏中的“询问”单选按钮，然后单击按钮。

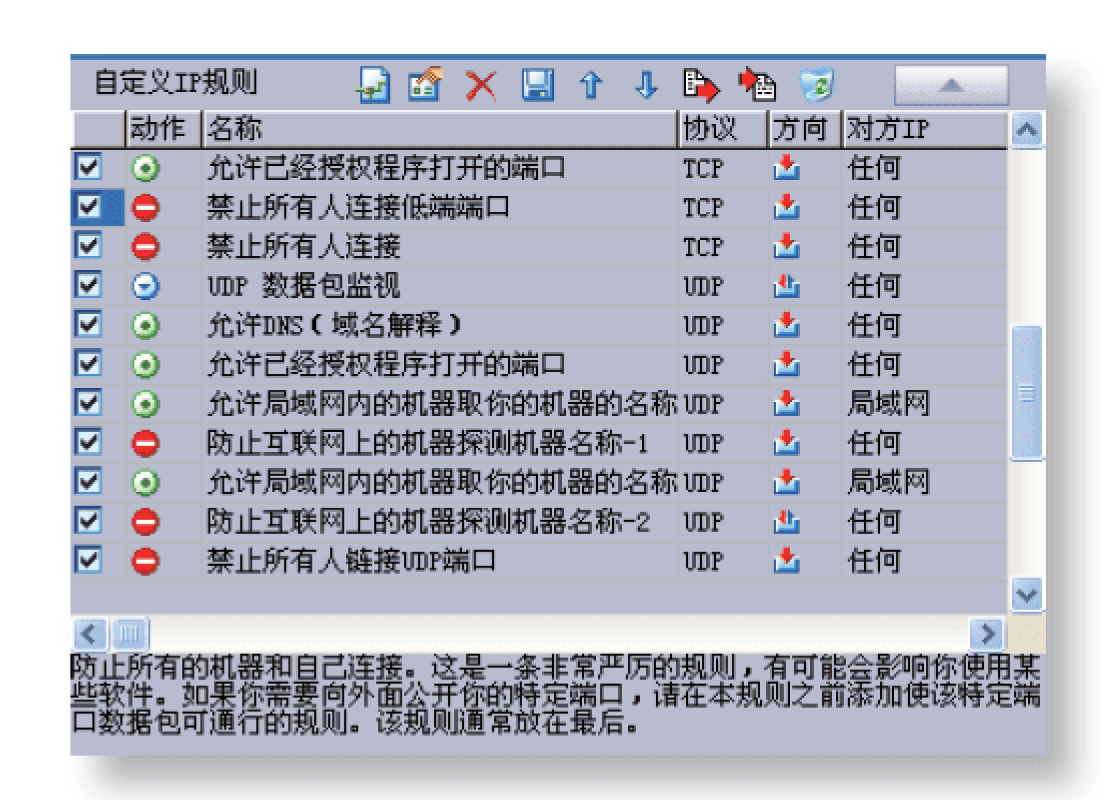




6.3.3 自定义IP规则

在天网防火墙中，可通过设置IP规则保证系统的安全性，防止黑客及不法人员对电脑的恶意入侵。灵活地设计适合用户自身使用的IP规则非常重要。

安全规则的设置是系统最重要也最复杂的地方。如果用户不熟悉IP规则，最好不要调整它，可以直接使用默认的规则。在天网防火墙的“自定义IP规则”对话框中，选中其中的某个复选框时，在其下方将显示对应规则的作用，以方便用户查看并进行合理的设置。





在天网防火墙个人版的主界面中单击按钮，即可打开“自定义IP规则”对话框，其中主要规则的含义如下。

- **禁止互联网上的用户使用电脑的共享资源：** 如开启该规则，则网络中其他用户将不能访问当前电脑上的共享资源，包括获取电脑名称。而“禁止所有人连接低端端口”则可以阻止所有的电脑和自己的低端端口连接。
- **防御ICMP攻击：** 启用该规则后，其他用户将无法用ping命令来确定用户电脑的存在。
- **允许已经授权程序打开的端口：** 使用QQ、FTP以及视频电话等软件时，系统都会开放相应的端口，才能保证其他用户准确地连接到本地电脑。通过启用该规则，可以保证这些软件的正常工作。
- **禁止所有人连接：** 该规则用于防止网络中其他电脑与本地电脑进行连接。这条规则仅适用于一些特殊的情况，有可能影响到该电脑中某些软件的使用，最好取消选中该复选框。
- **UDP数据包监视：** 通过该规则，可监视电脑与外部网络之间的所有UDP包的发送和接收过程。

教你一招

UDP数据包监视的使用情况

“UDP数据包监视”规则开启后会产生大量的日志，因此通常不启用该规则。熟悉TCP/IP网络协议的用户可使用该规则进行数据监测，如对网络不熟悉，建议不要启用该规则。

6.3.4　使用瑞星防火墙

使用瑞星防火墙可对网络攻击、恶意网址以及IP规则进行设置，达到拦截网络威胁、保护电脑安全的目的。



下面将使用瑞星防火墙设置网络攻击拦截、恶意网址拦截和IP规则，其具体操作如下。

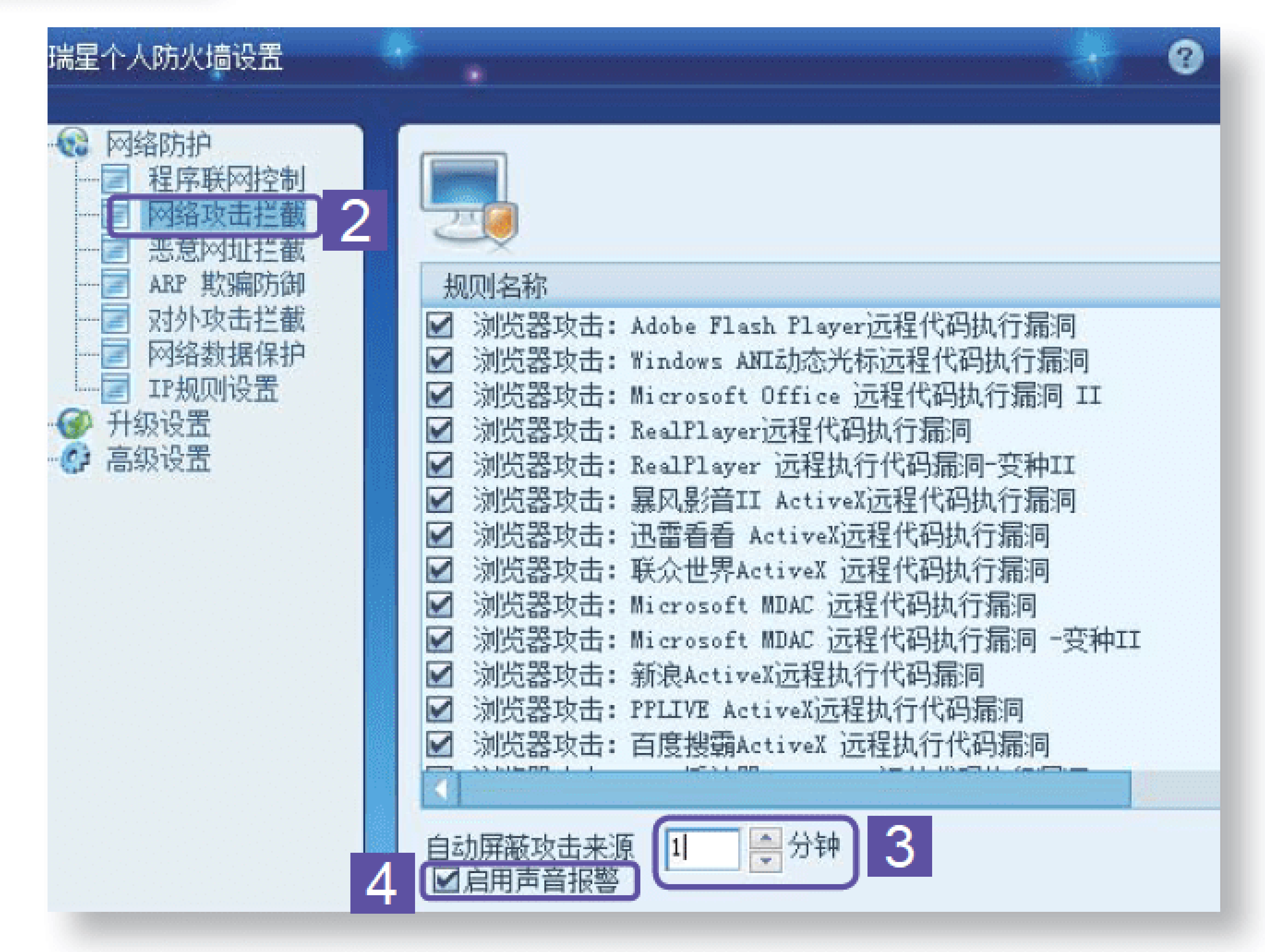


第1步：进入瑞星防火墙设置界面

安装并启动瑞星防火墙，在其主界面中可查看其网络防护状态，单击“设置”超链接，即可进入瑞星个人防火墙的设置界面。

第2步：设置网络攻击拦截

在打开界面的左侧窗格中展开“网络防护”选项，选择“网络攻击拦截”选项，在其右侧窗格中将“自动屏蔽攻击来源”数值框中的时间设置为1，然后选中“启用声音报警”复选框。





第3步：设置恶意网址拦截

选择“恶意网址拦截”选项，在其右侧窗口中单击“添加”超链接，添加IE浏览器选项，然后选中“启用钓鱼网页扫描功能”和“启用搜索引擎搜索结果风险分析”复选框。





第4步：设置IP规则

选择“IP规则设置”选项，在其右侧窗格的列表框中选中允许放行的选项前的复选框，然后单击 确定(O) 按钮应用设置。

跟我练习

配置天网防火墙相关应用程序规则

任务1：为了防止别人更改天网防火墙的规则，设置管理员密码以确保其安全。

任务2：设置应用程序Outlook Express在网络中的访问权限，以保证安全接收网络中的邮件。



设置管理员密码



设置应用程序规则

6.4 防火墙的选择

阿伟为娜娜讲解了在个人电脑中设置防火墙的方法和步骤，娜娜已经能熟练地操作了。但当她想到现在的防火墙产品数不胜数时，又困惑了，不知道选择怎样的防火墙产品才更安全可靠。娜娜将自己的疑惑告诉阿伟，想让阿伟为她解惑。

6.4.1 防火墙的种类

防火墙可以根据不同的划分标准进行分类，这里主要对其从软硬件形式、结构和技术方面的分类进行讲解。

1. 根据软硬件形式进行分类

从防火墙的软、硬件形式来分，主要可分为软件防火墙、硬件防火墙和芯片级防火墙3类。



下面将分别对其进行介绍。



名称：软件防火墙

特点：软件防火墙运行于特定的电脑上，它需要电脑操作系统的支持，一般来说这台电脑就是整个网络的网关，俗称“个人防火墙”。软件防火墙就像其他的软件产品一样需要先在电脑中安装并做好配置才可以使用，如瑞星防火墙。

名称：硬件防火墙

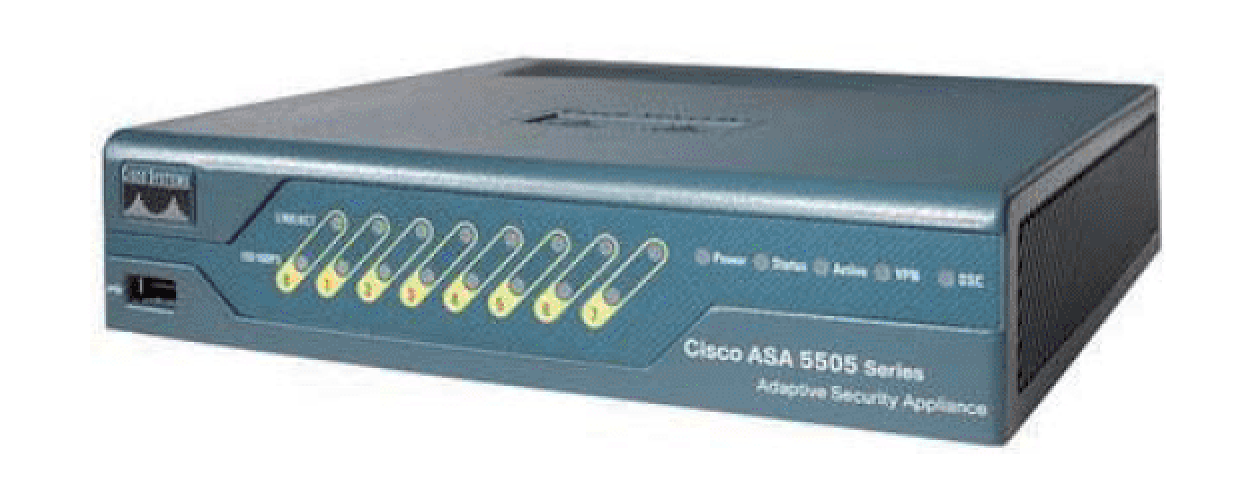
特点：目前市场上大多数硬件防火墙都与电脑相似，它们和普通的家用电脑没有太大区别。在这些PC架构电脑上运行一些经过裁剪和简化的操作系统。现在一些新的硬件防火墙扩展了端口，四端口防火墙一般将第四个端口作为配置和管理端口。





名称：芯片级防火墙

特点：芯片级防火墙只需通过硬件实现防火墙功能，没有操作系统。专有的芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。这类防火墙最出名的厂商有NetScreen、FortiNet、Cisco等。这类防火墙本身的漏洞比较少，不过价格相对比较高昂。



2. 根据防火墙结构进行分类

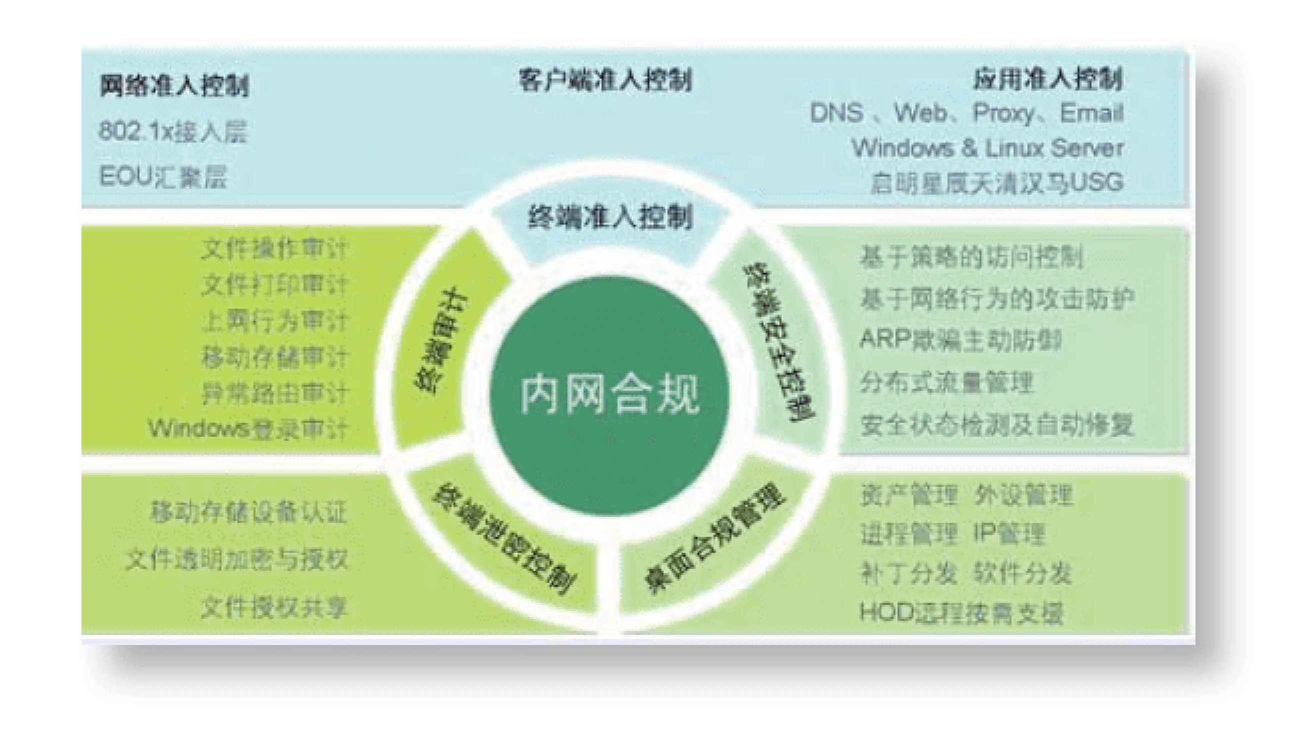
从防火墙结构上分，主要可分为单一主机防火墙、分布式防火墙和路由器集成式防火墙3类。

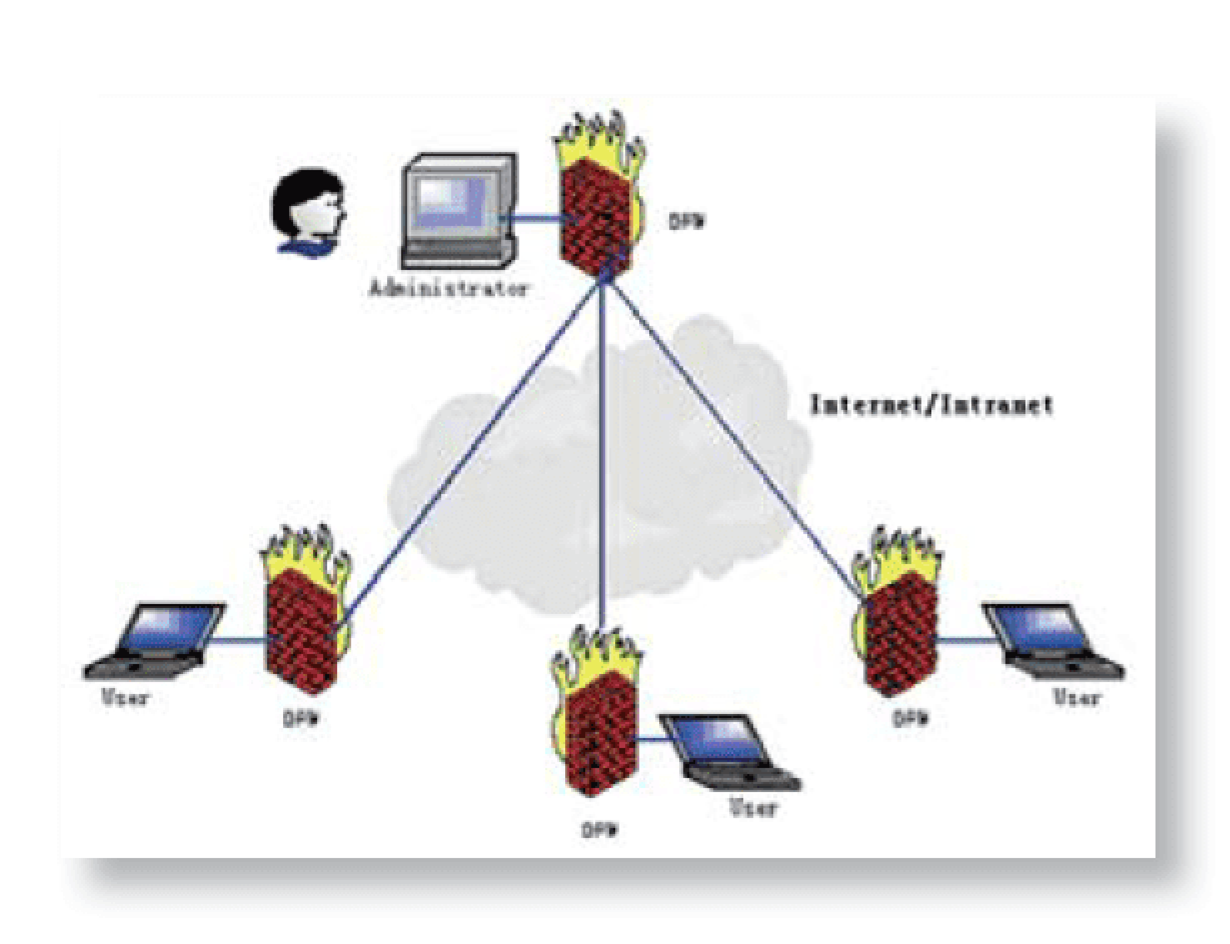


下面将分别对其进行介绍。

名称：单一主机防火墙

特点：这种防火墙与一台电脑的结构类似，它与一般电脑最主要的区别就是集成了两个以上的以太网卡，因为它需要连接一个以上的内、外部网络。其工作性质决定了其要具备非常高的稳定性、实用性，具备非常高的系统吞吐性能。正因如此，看似与电脑类似的配置，价格却高出很多。





名称：分布式防火墙

特点：分布式防火墙不再是位于网络边界，而是渗透于网络的每一台主机中，对整个内部网络的主机实施保护。在网络服务器中，通常会安装一个用于防火墙系统管理的软件，在服务器及各主机上安装有集成网卡功能的防火墙卡，这样一块防火墙卡同时兼有网卡和防火墙的双重功能。这样一个防火墙系统就可以彻底保护内部网络。



名称：路由器集成式防火墙

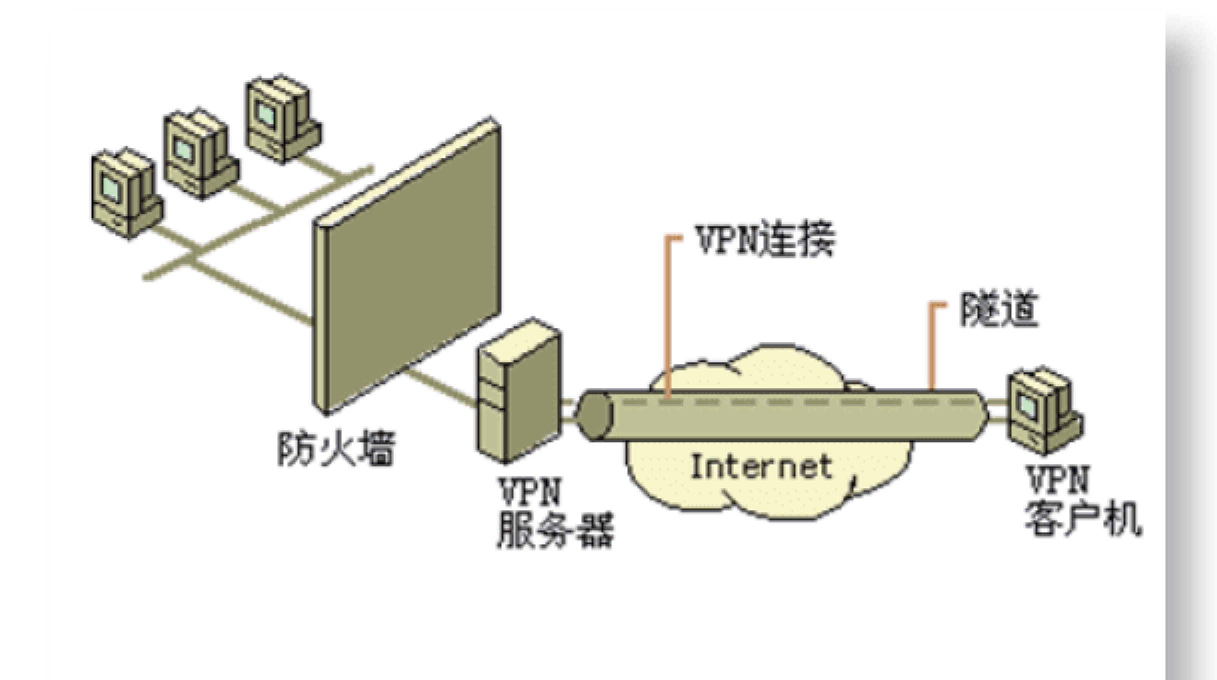
特点：路由器集成式防火墙不仅可以有效防止网络受到病毒入侵和黑客的攻击，还可以灵活地组合成一系列控制规则，形成一套完整的控制策略，既可以有效管理用户的上网权限，又能方便地对局域网中的电脑进行进一步管理。

3. 根据防火墙技术进行分类

防火墙技术虽然出现了许多，但总体来讲可分为包过滤型和应用代理型两大类。



下面将分别对其进行讲解。



名称：包过滤型防火墙

特点：包过滤方式是一种通用、廉价且有效的安全手段。其通用性主要表现在它不是针对各个具体的网络服务采取特殊的处理方式，而是适用于所有网络服务；其廉价性主要表现在大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；其有效性主要表现在它能在很大程度上满足绝大多数企业安全要求。

新手解惑

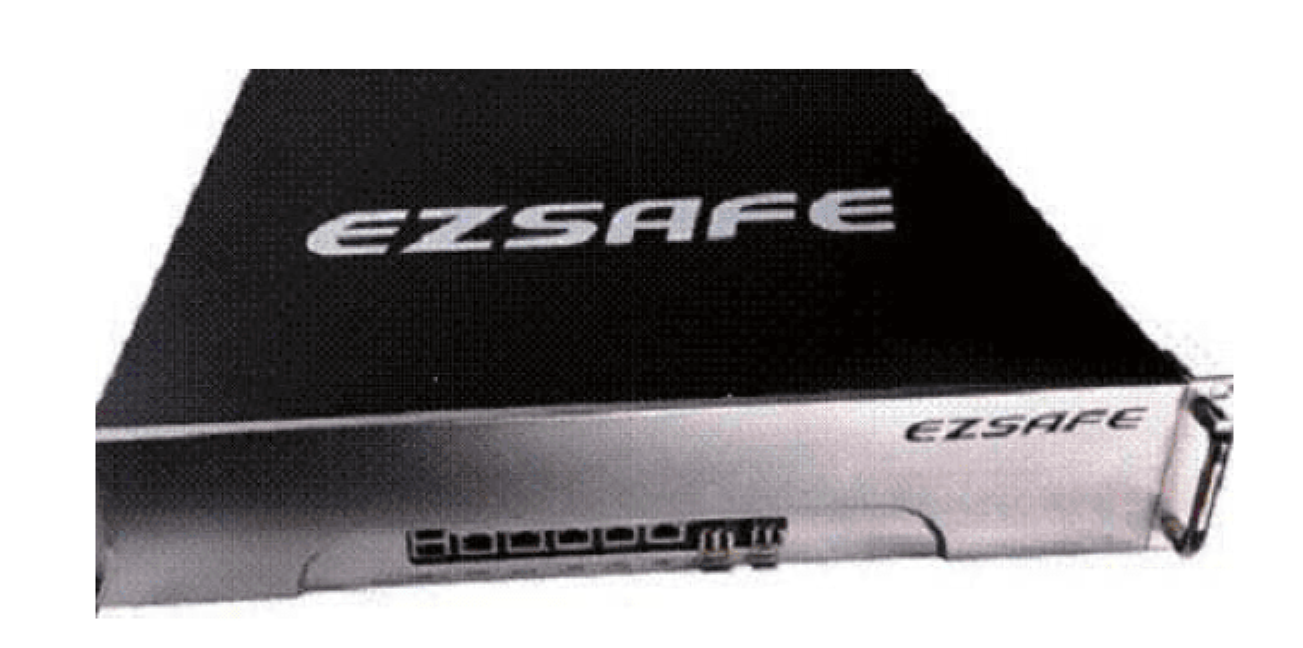
Q：第一代静态包过滤型防火墙和第二代动态包过滤型防火墙的特点分别是什么？

A：第一代静态包过滤型防火墙是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括IP源地址、IP目标地址、传输协议、TCP/UDP目标端口和ICMP消息类型等。第二代动态包过滤型防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所存在的问题。



名称：应用代理型防火墙

特点：代理型防火墙最突出的优点就是安全。它工作于最高层，因此可以对网络中任何一层的数据通信进行筛选保护。代理型防火墙采用一种代理机制，可以为每一种应用服务建立一个专门的代理，所以内外部网络之间的通信不是直接的，而是需先经过代理服务器的审核。



新手解惑

Q：第一代应用网关型防火墙和第二代自适应代理防火墙的特点分别是什么？

A：第一代应用网关型防火墙通过代理技术参与到一个TCP连接的全过程，隐藏了内部网结构。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙，其核心技术就是代理服务器技术。第二代自适应代理防火墙是一种新防火墙类型，它可以结合代理型防火墙的安全性和包过滤型防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高10倍以上。

6.4.2 防火墙选择的误区

目前，虽然用户对于网络安全都有需求，但是对于如何选择网络安全产品——防火墙，却存在着很多误区。



选择防火墙通常存在以下几个误区。

- **国外的防火墙就一定好：**在国内进行的多次评测中，国内防火墙产品在性能指标上和国外的产品各有千秋。国外的防火墙往往是一个方面突出；国内的防火墙其优势在于功能全面、易用且服务本地化。片面强调一个功能对防火墙来说是不够的，用户应该结合自身的实际需求选择防火墙。
- **纯硬件防火墙比软件防火墙好：**一般情况下，要实现防火墙的功能主要还是通过软件。硬件防火墙在需要添加功能时实现比较困难，而在软件防火墙上则可很容易地进行添加，甚至可以应用户的要求制定开发。

- **防火墙的各项指标越高越好：** 其实还是那句话，按需选择。在用户资金有限的情况下，还是应该仔细衡量一下哪些指标对用户来说更有用。当然，选择产品时一定要有前瞻性，产品最好能适应今后几年内网络的扩展需要。
- **CPU越快越好，内存越大越好：** 防火墙不是服务器，因为各种防火墙实现原理不同，所以靠CPU和内存来衡量是片面的，具体还要看其指标。

6.4.3 选择防火墙时需考虑的问题

防火墙不同于路由器、交换机和服务器，因此，不能用这些产品的指标来选择防火墙。那么选择防火墙应该注意哪些方面呢？



下面将对选择防火墙时应注意的问题进行介绍，主要包括如下几点。

1. 安全性

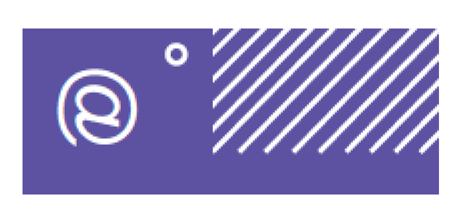
安全性不高的防火墙，其他性能再好也是空谈。防火墙的安全性包括自身安全性、访问控制能力和抗攻击能力3个方面。自身安全性主要是指防火墙系统的健壮性，也就是说防火墙本身应该是难以被攻入的。访问控制能力是防火墙的核心功能，访问控制能力包括控制细度，也就是能控制哪些内容。抗攻击能力指防火墙对各种攻击的抵抗能力，包括能抵御的攻击种类和数量。

2. 网络功能

防火墙的网络功能包括地址转换、IP/MAC绑定、静态和动态路由 、源地址路由、代理、透明代理、ADSL拨号、DHCP支持、双机热备和负载均衡等。并不是每一个功能用户都需要，因此，用户应该首先明确自己需要什么功能，并且要确定这些功能都要达到什么效果，然后再寻找相应的设备。有些功能在不同厂家的定义里是不同的，实现的效果也不一样。

3. 网络性能

在保证安全的基础上，防火墙应能最大程度地减少对网络性能的影响。对于网络性能，主要就是看最大带宽、并发连接数、每秒新增连接数、丢包和延迟等指标。这些指标和交换机、路由器是相同的。但需要注意的是，防火墙在策略起作用和全通策略的不同状态中，上述指标是不一样的，用户应考虑实际环境的需求。



4. 管理功能

防火墙需要经常管理。日常的管理就是看日志、修订策略以及添加和删除用户。更高的管理还包括第三方互动、VPN建立、远程集中管理等。管理方面用户应该注意界面的友好性，设置选项应该通俗易懂。日志特别重要，好的日志系统应该有详细的记录，应该便于分类和排序，应该方便存入数据库。



考虑防火墙的性价比

选择防火墙时，除要考虑以上因素外，用户还应考虑防火墙的用途，并根据其使用的地方选择性价比较高的防火墙。

6.4.4 个人防火墙的选择标准

对于个人用户来说，防火墙软件的选择不必像服务器以及大型网络系统的防火墙那样，以安全防御能力为首要条件，而应从安全防御能力、易用性和软件稳定性等多个方面来均衡考虑。



下面将对防火墙的安全防御能力、易用性和软件稳定性方面进行介绍。

- **安全防御能力：** 防火墙软件功能的基本要求是对网络通信协议和通信端口进行限制，阻断可能的入侵途径。但面对日益严峻的网络安全问题，这种安全防御模式明显是不够的，还需要防火墙有其他更灵活的安全技术。
- **易用性：** 许多附加功能对于个人用户的意义也很大，如让程序经许可之后才可运行的程序控制功能、根据程序的特征判断是否为特洛伊木马的功能等。此外，还有对于个人用户网络安全影响重大的隐私保护功能。
- **软件稳定性：** 除了安全防御能力以外，防火墙软件自身的稳定性也应该列入考虑的范围。软件功能多，通常会影响到软件的稳定性，同时占用的系统资源也将更多，设置和管理的难度也会相应提高。个人用户应以适用和够用为原则，不必盲目地迷信企业版防火墙软件。实际上，大型网络系统多以数据包过滤型硬件设备为第一道安全防线，因此企业版防火墙对个人用户并不适用。

6.5　更进一步——防火墙的秘密

通过阿伟的讲解，娜娜知道了防火墙在电脑中的重要性，并且掌握了在电脑中开启系统自带防火墙以及使用天网防火墙为网络设置规则的方法。娜娜很感激阿伟，于是想当面感谢他。正好阿伟想要给娜娜讲解几个防火墙方面的小技巧，于是娜娜又学到了一些新的知识。

第1招　创建FTP共享规则



提示：FTP是用于在两台装有不同操作系统的电脑中传输用户文件的一个软件标准，使用其可以实现文件的共享。

在Windows防火墙中创建FTP的入站规则可对FTP的共享功能进行限制。其方法如下：

①在控制面板中单击“Windows 防火墙”超链接，在打开窗口的“入站规则”按钮上单击鼠标右键，在弹出的快捷菜单中选择“新建规则”命令。

②在打开的向导中选中“端口”单选按钮，单击 下一步(N) > 按钮，在打开的“协议和端口”向导中选中“特定远程端口”单选按钮，在其后的文本框中输入“21”，单击 下一步(N) > 按钮。

③在打开的向导中选中“允许连接”单选按钮，然后依次单击 下一步(N) > 按钮，完成规则的创建。

第2招　Windows 7防火墙的新程序提示



在Windows 7防火墙设置中，启用防火墙后，可在其下方选中“Windows 防火墙阻止新程序时通知我”复选框，这样用户就能在新程序启动时及时得到系统提示。如果选中“阻止所有传入连接，包括位于允许程序列表中的程序”复选框，则会影响用户对电脑的使用。



第3招 使用天网防火墙的设置向导



在安装天网防火墙时，安装程序将在安装的过程中启用设置向导，用户可根据自身的需要进行相关配置，其方法如下：

①运行天网防火墙安装程序，当程序安装后将打开其设置向导，在打开的“安全级别设置”对话框中选中“高”单选按钮，单击[下一步]按钮。

②在打开的“局域网信息设置”对话框中可对电脑的IP地址进行设置，完成后防火墙将应用该设置。

第4招 使用瑞星防火墙网络防护功能



瑞星防火墙是目前功能较完善的防火墙，用户可使用其进行网络防御并设置相关的IP规则，还能对电脑中的应用程序进行管理。其设置方法如下：

①安装并启动瑞星防火墙，在其主界面中选择“网络防护”选项卡，在其下方将出现各种网络防护功能。

②选择相应的选项，单击其右侧的[设置]按钮，在打开的对话框中进行相应的设置，完毕后瑞星防火墙即开始对电脑进行安全防护。

6.6 活 学 活 用

（1）简述防火墙的功能，并上网查找你的个人电脑中使用的防火墙类型、特点以及主要功能。

（2）开启电脑的Windows防火墙功能，并对相关应用程序设置允许通过的程序及功能。

（3）使用Windows防火墙高级设置，创建入站规则及出站规则，允许相应电脑中的杀毒软件进行网络连接。



入站规则

名称	组	配置文件	已启用	操作	替代
360安全卫士实时保护		专用	是	允许	否
360安全卫士实时保护		公用	是	允许	否
360安全卫士实时保护		公用	是	允许	否
360安全卫士实时保护		专用	是	允许	否
KwMusic		专用	是	允许	否
KwMusic		专用	是	允许	否
LiveUpdate360		公用	是	允许	否
LiveUpdate360		公用	是	允许	否
LiveUpdate360		专用	是	允许	否
LiveUpdate360		专用	是	允许	否
MazeSvr		专用	是	允许	否
MazeSvr		专用	是	允许	否

（4）下载并安装天网防火墙，使用其对电脑中的应用程序进行IP规则的设置，保证使用的安全性。

（5）简述选择防火墙的误区以及个人防火墙的选择方法。



- ☑ 想知道怎么保障Internet信息的安全性吗？
- ☑ 还在为使用IE浏览器弹出垃圾广告而烦恼吗？
- ☑ 想知道怎样避免收到垃圾邮件吗？
- ☑ 还在为使用QQ和MSN聊天的安全而担心吗？



第 07 章 网络信息安全设置

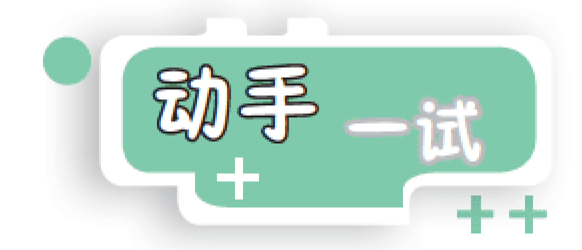
娜娜今天很不高兴，因为她的QQ被盗了，而且不能打开网页，她担心自己的聊天记录被别人知道了，那可是有很多她和朋友之间的秘密啊。不过现在也没办法了，只有找到阿伟寻求帮助，将电脑进行全面的安全设置，让以后使用网络传递信息时更安全。阿伟很热情地帮助娜娜解决这个问题。

7.1　设置Internet选项

阿伟告诉娜娜，在使用电脑上网时，大部分的操作是在浏览器中进行的，因此，设置Internet的安全性非常重要。娜娜听了以后似懂非懂，于是问道：“那是不是前面你教我的那些设置呢？”阿伟回答道：“当然不是啊，现在就教你一些简单有效的设置。”

7.1.1　设置Internet安全级别

在“Internet 选项”对话框中用户可进行安全级别设置，避免在上网过程中无意识地打开包含病毒和木马程序的网页或下载到带病毒的文件，从而感染电脑。



下面将对设置Internet安全级别进行讲解，其具体操作如下。

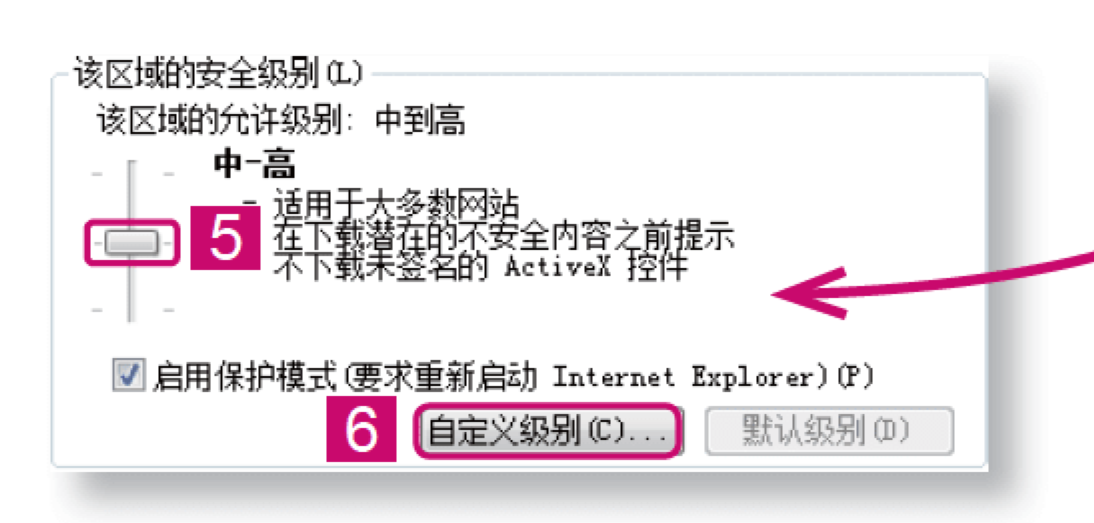


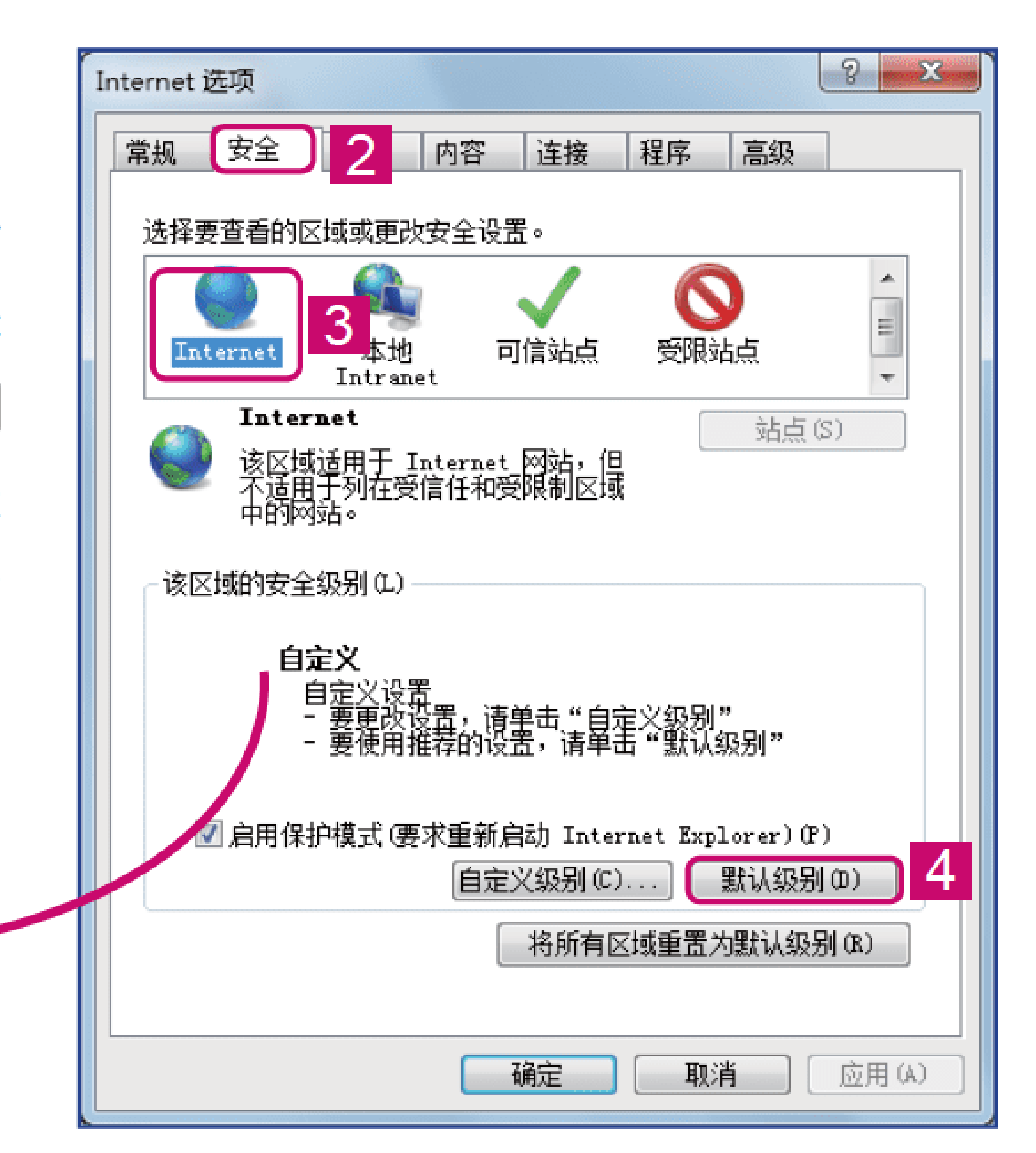
第1步：打开“Internet 选项”对话框

双击桌面上的图标，在打开的浏览器窗口中选择“工具”/“Internet 选项”命令，打开“Internet 选项”对话框。

第2步：选择Internet安全级别

选择“安全”选项卡，在“选择要查看的区域或更改安全设置”列表框中选择Internet选项，然后在下方单击默认级别(D)按钮，此时将显示设置滑块，拖动滑块即可设置Internet的安全级别。然后单击自定义级别(C)...按钮。

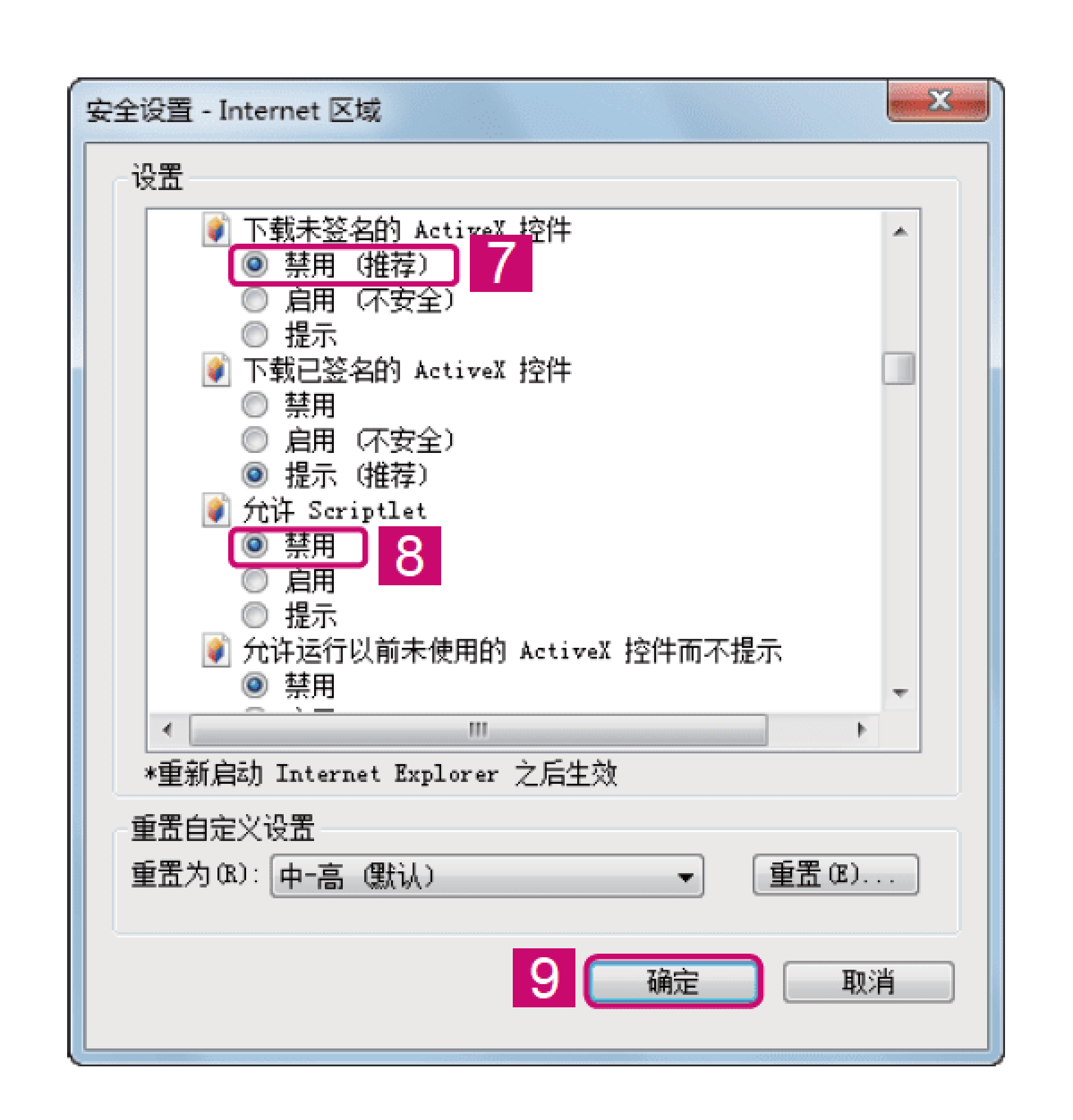


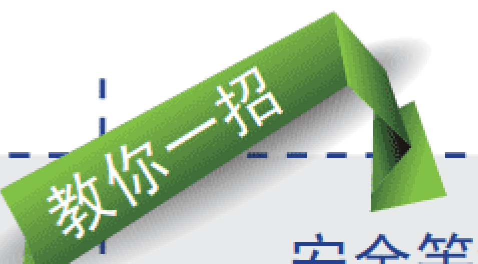




第3步：自定义安全选项

在打开对话框的“设置”列表框中设置相关安全选项，这里将“下载未签名的AxtiveX控件”和“允许Scriptlet”等选项禁用，完成设置后，依次单击确定按钮即可。





：使用拖动滑块的方法比自定义设置更快捷，但使用自定义设置能准确地设置其安全选项，用户可根据实际情况进行设置。

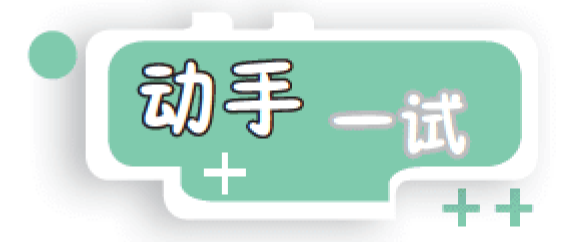
教你一招

安全等级的使用

通常情况下，用户在进行安全级别的设置时应选用默认的“中-高”或“中”级别，而不使用“高”级别，使用“高”将导致无法下载文件或网银不能正常使用的情况。

7.1.2 设置可信站点

在“Internet 选项”对话框中用户可将需经常访问的或确定无安全隐患的网站设置为可信任站点，以便用户的正常访问。



下面将对设置可信任站点的方法进行讲解，其具体操作如下。

第1步：打开“可信站点”对话框

打开“Internet 选项”对话框，选择“安全”选项卡，然后在其列表框中选择“可信站点”选项，单击站点(S)按钮，打开“可信站点”对话框。





第2步：设置可信站点

在打开对话框的“将该网站添加到区域”文本框中输入要添加的站点网址，这里输入“https://www.baidu.com”，单击添加(A)按钮即可添加信任网站，然后依次单击关闭(C)按钮。

提示：除了设置信任站点能提高上网的安全性外，还可以设置受限站点，将有可能危害电脑或文件的站点添加到其中，其方法与添加信任站点相同。

7.1.3 删除临时文件

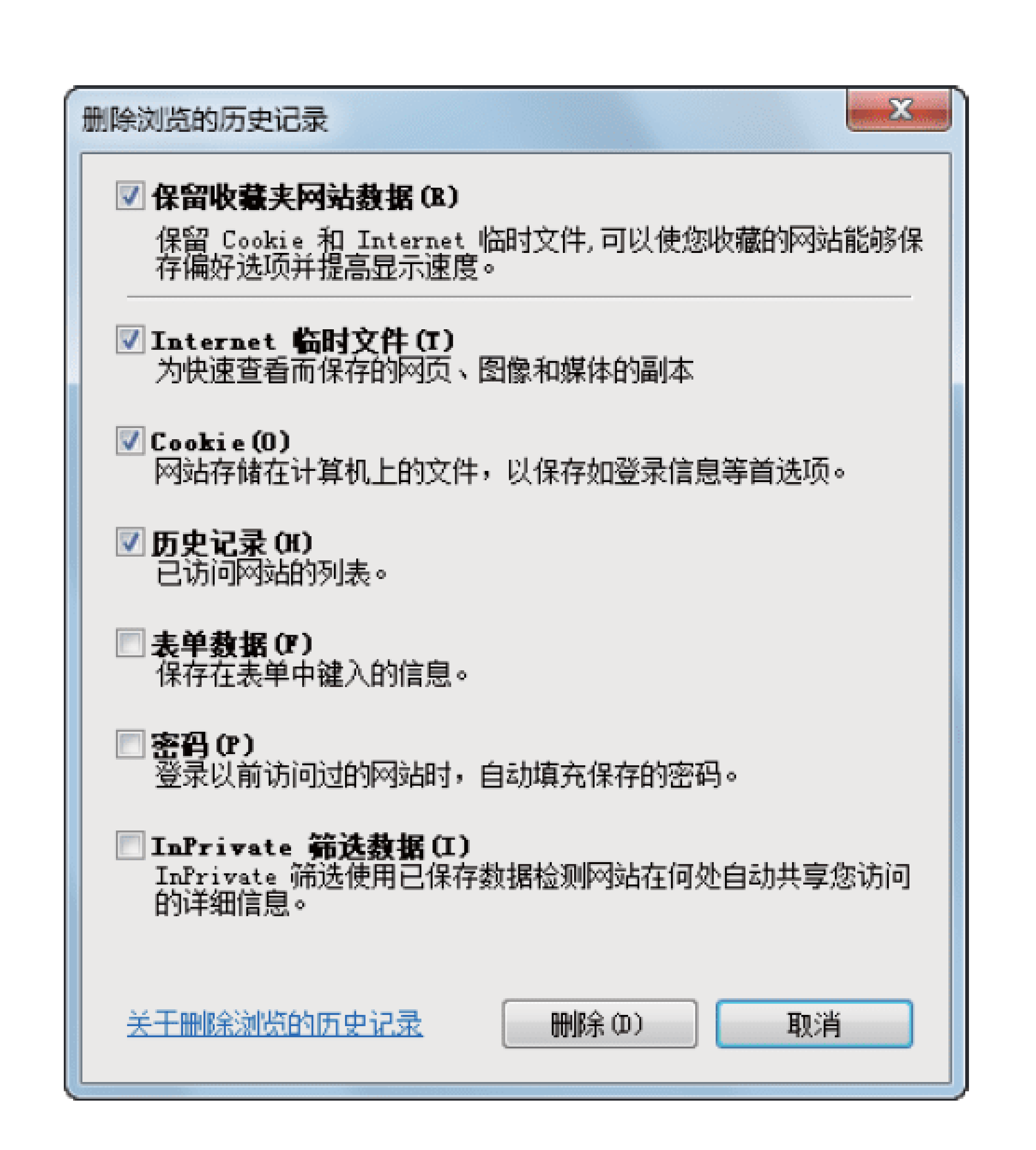
临时文件夹中存放着用户访问过的网站的相关信息，这些信息可能会泄露用户的个人隐私。因此，在使用电脑一段时间后，应删除临时文件，这样不但可以保护用户信息，也可释放磁盘空间。



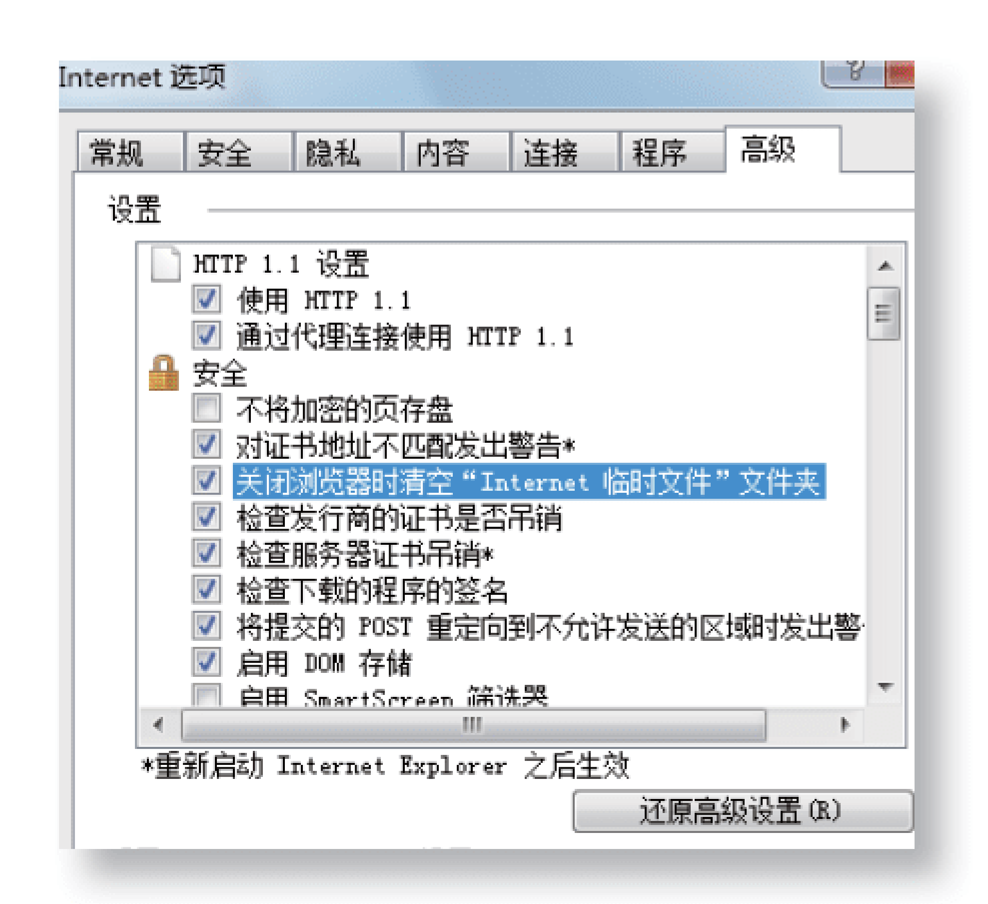
删除临时文件可通过手动删除，也可设置自动删除，下面分别对其进行讲解。

1. 手动删除临时文件

打开“Internet 选项”对话框，选择“常规”选项卡，单击“浏览历史记录”栏中的删除(D)...按钮，打开“删除浏览的历史记录”对话框，在此对话框中系统将默认选中要删除的临时文件前的复选框，然后单击删除(D)...按钮将删除系统产生的临时文件。



提示：不同版本的IE浏览器其删除临时文件的方法类似，都可以在“Internet选项”对话框中进行。



2. 设置自动删除临时文件

打开“Internet选项”对话框，在其中选择“高级”选项卡，在“设置”列表框的“安全”栏中选中“关闭浏览器时清空‘Internet临时文件’文件夹”复选框，单击 确定 按钮应用设置。

教你一招

为了能更快捷地清除系统临时文件，阿伟教娜娜制作清除垃圾文件的批处理文件，只需运行该文件，系统中的“垃圾”将被清除。

新建一个文本文档，然后将其代码复制到该文本文件中，保存后关闭文件，将其后缀名“.txt”修改成“.bat”即可。

删除系统临时文件的代码如下：

```
@echo off
echo 正在清除系统垃圾文件，请稍等......
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\temp\*.*
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.*"
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成！
echo. & pause
```

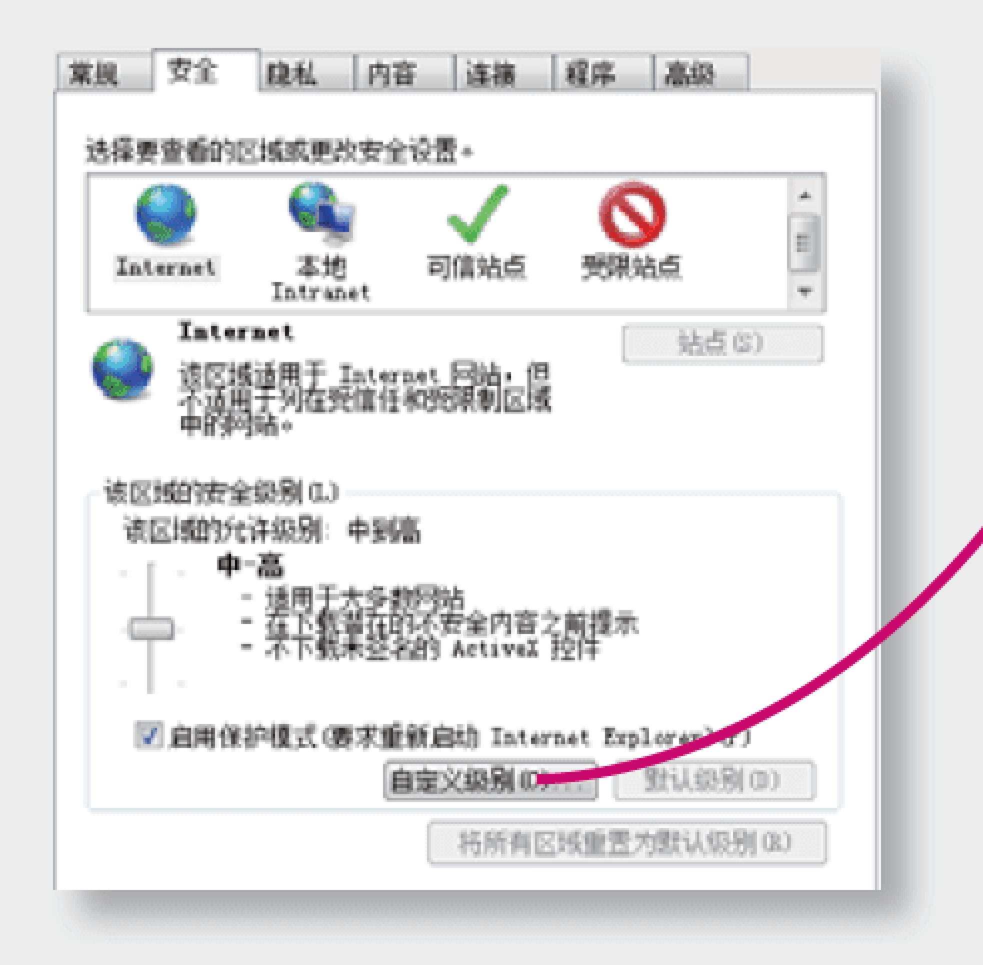
跟我练习

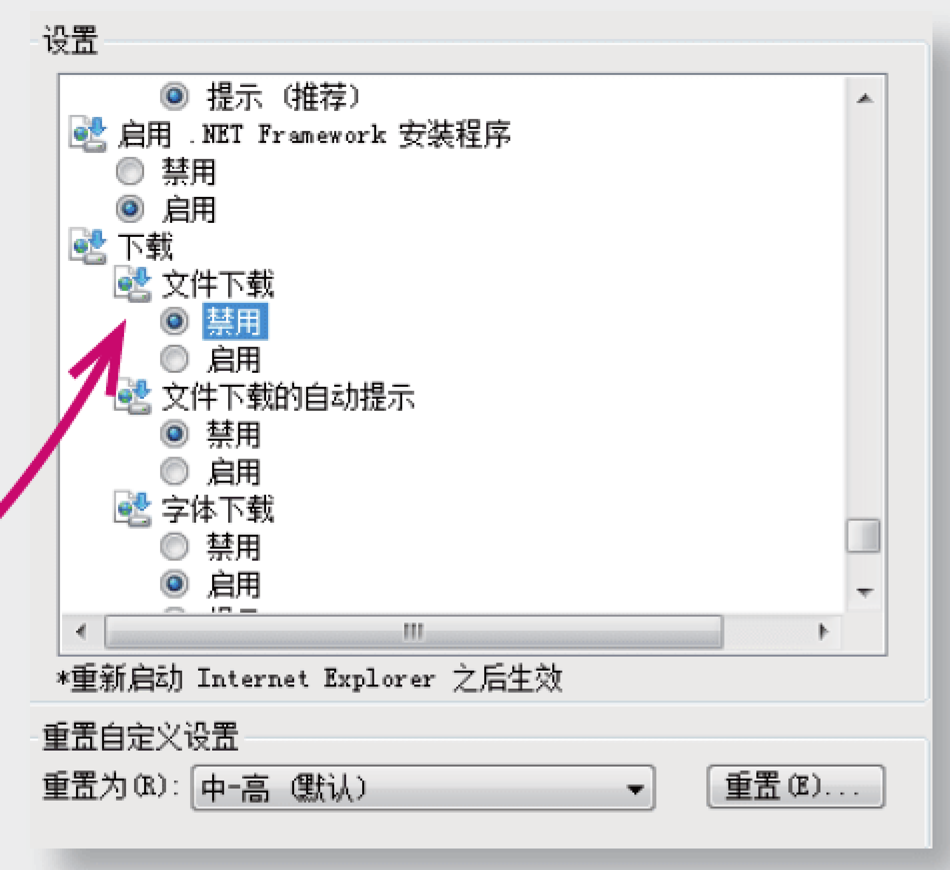
设置Internet选项，使用户在连接Internet上网时能保证其安全性

任务1：打开“Internet 选项”对话框，在“安全”选项卡中设置其安全级别。

任务2：设置可信站点，并在“常规”选项卡中单击 删除(D)... 按钮，在打开的对话框中删除历史记录。

任务3：打开“Internet 选项”对话框，在“安全”选项卡中单击 自定义级别(C)... 按钮，在打开的对话框中将“文件下载”选项禁用。





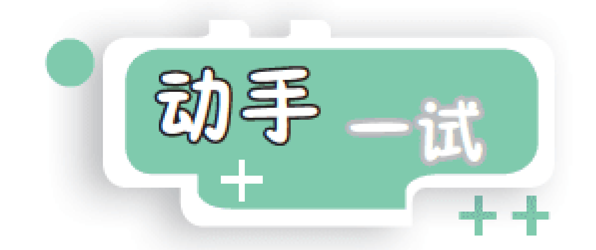
7.2 使IE浏览器上网更安全

通过阿伟的讲解，娜娜不仅对上网的安全性有了更加清晰的认识，而且能够进行简单的设置，但是她还存在着很多疑问，于是又找到阿伟，请教阿伟关于其他更多的关于IE安全的设置。

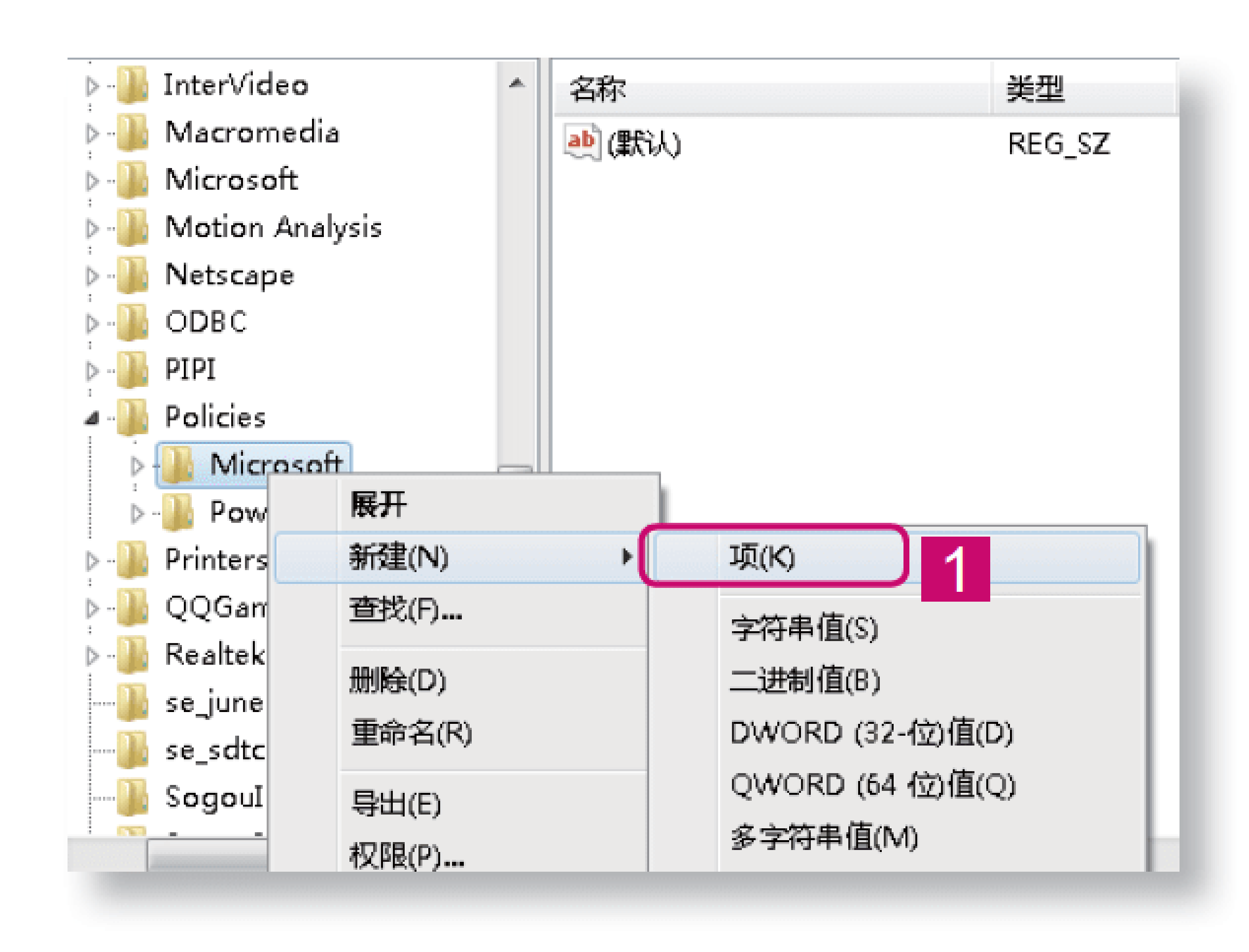
7.2.1 隐藏IE属性选项卡

“Internet 选项”对话框中的选项卡对设置IE浏览器的属性与保护网络信息的安全有着非常重要的作用，为防止其他用户修改其中的内容，用户可以将相应的选项卡进行隐藏，从而保证其安全。





这里以隐藏“安全”选项卡为例进行讲解，其具体操作如下。



第1步：新建项

打开注册表编辑器，在其左侧窗格中展开HKEY_CURRENT_USER/Software/Policies/Microsoft选项，在Microsoft选项上单击鼠标右键，在弹出的快捷菜单中选择“新建”/“项”命令，将新建项的名称设置为Internet Explorer，按相同方法在其下新建Control panel选项。

第2步：新建DWORD值

在右侧窗格空白处单击鼠标右键，在弹出的快捷菜单中选择“新建”/“DWORD（32位）值”命令，将新建的DWORD值名称设置为SecurityTab，双击该键值，在打开的对话框中设置其数值数据为1，单击 确定 按钮。



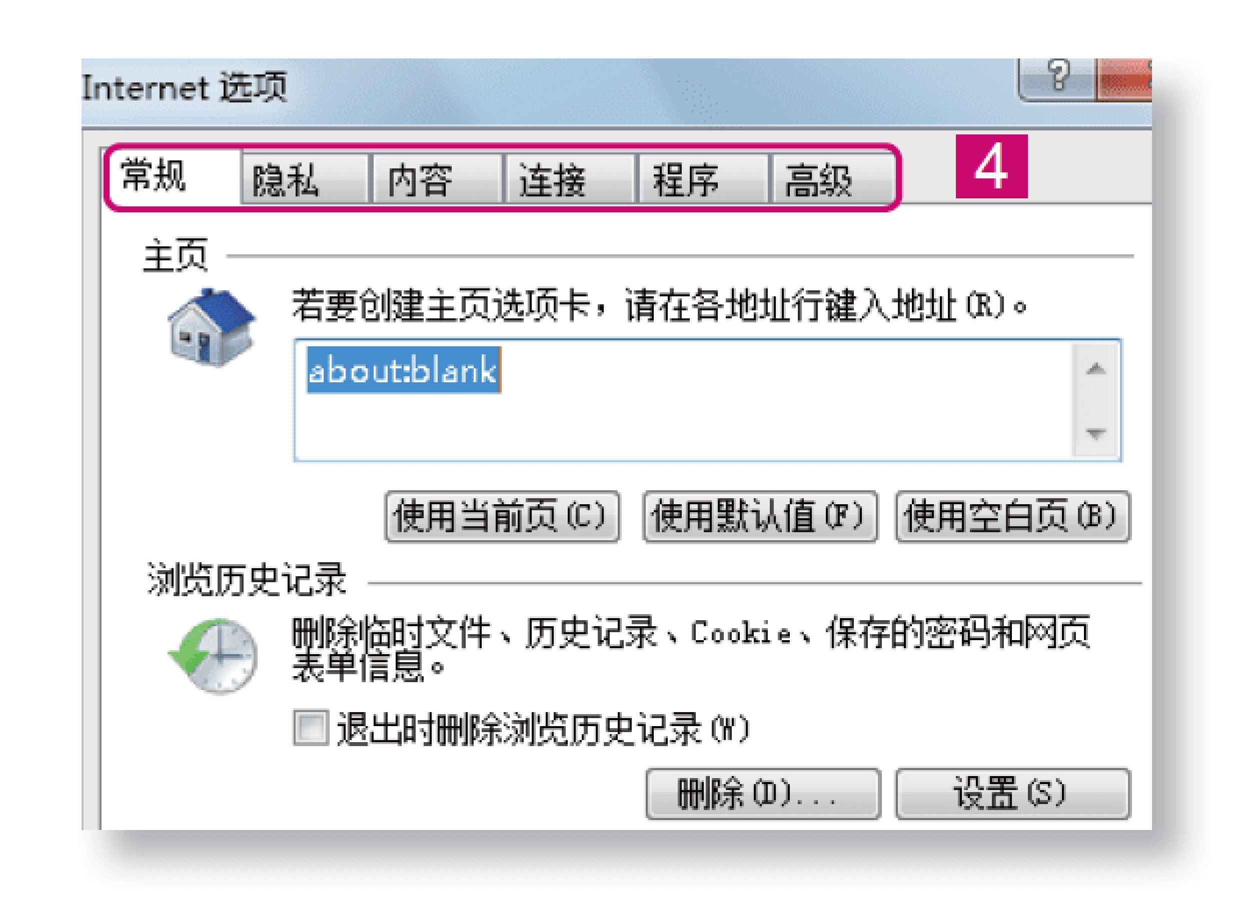
教你一招

Word值的基数设置

通常在注册表中新建Word值后，要启用或禁止该值，在打开的对话框中只需设置其“数值数据”即可，将该值的基数保持默认设置，即选中“十六进制”单选按钮。

第3步：查看隐藏效果

完成操作后，重新打开“Internet 选项”对话框，即可看到“安全”选项卡已被隐藏。若想隐藏其他选项卡，只需在右侧窗格中继续新建DWORD值，然后将其进行重命名，并将值修改为1即可。



提示：如要显示隐藏的选项卡，只需将对应的DWORD值删除或将其数值数据改为0。

“Internet 选项”对话框中选项卡对应的注册表DWORD值

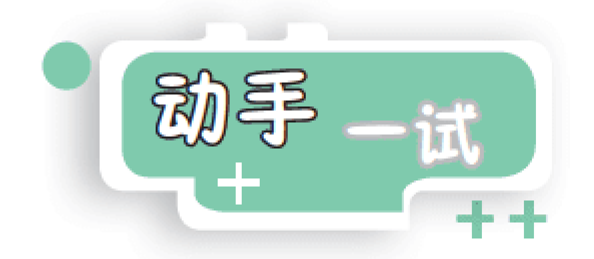
选项卡名称	DWORD值名称
常规	GeneralTab
隐私	PrivacyTab
内容	ContentTab
连接	ConnectionsTab
程序	ProgramsTab
高级	AdvancedTab

7.2.2 禁用更改浏览器的主页

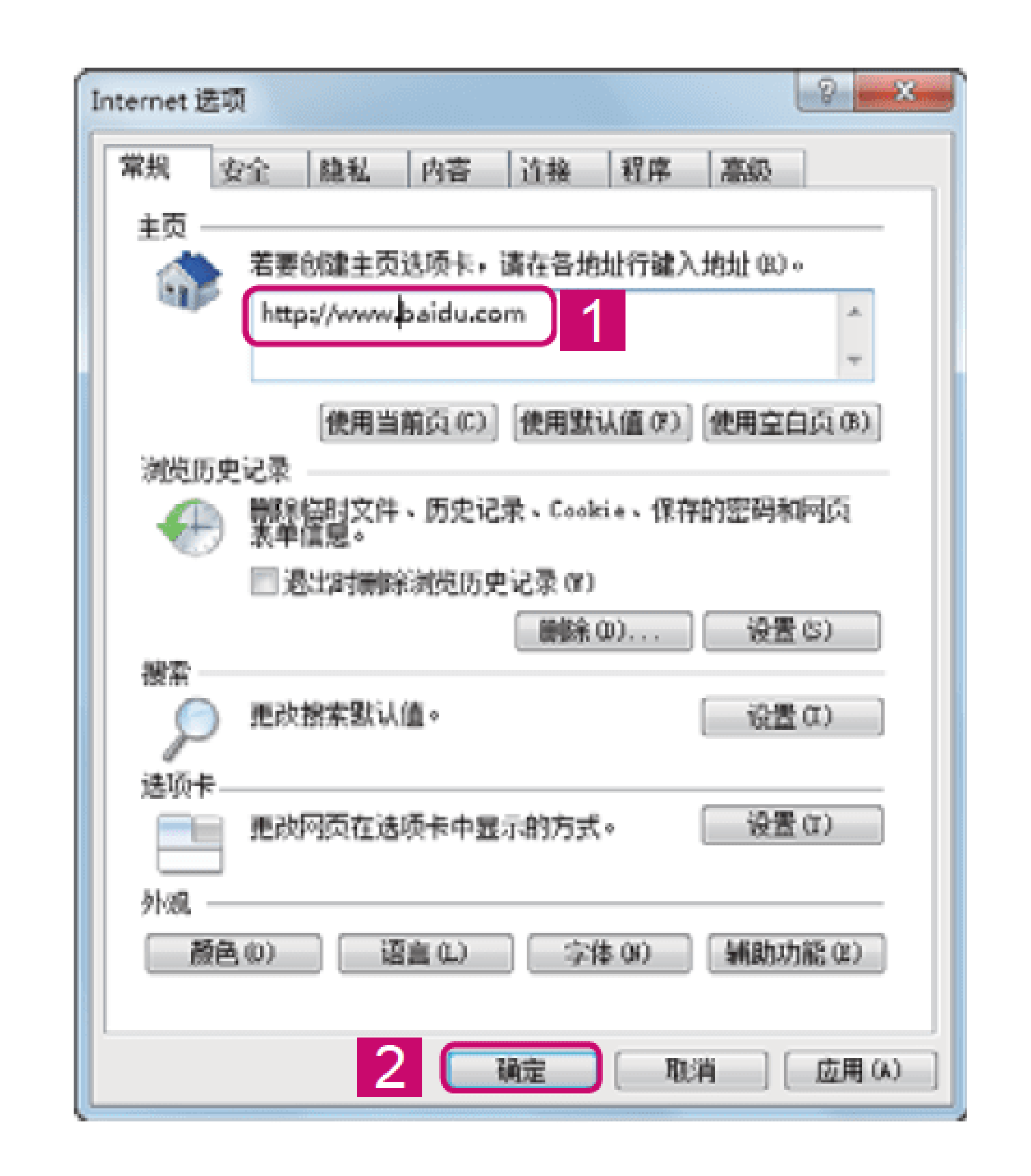
在浏览网页的过程中，经常会发现恶意网页修改了IE浏览器的默认主页地址，当其被修改后，将自动链接恶意网页，即使在“Internet 选项”对话框中对主页地址进行修改也无济于事，这时可以通过注册表和组策略禁用设置浏览器主页来解决。

1. 通过注册表禁止

禁止更改浏览器主页后，将不能更改“Internet 选项”对话框中要打开主页的地址，用户可在禁用前进行设置。



下面将对在注册表中禁用更改浏览器主页功能的方法进行简单讲解，其具体操作如下。



第1步：设置要打开的主页

启动浏览器，然后选择“工具”/“Internet选项”命令，在打开对话框的列表框中输入“http://www.baidu.com”，然后单击 确定 按钮保存设置。

提示：也可以将主页设置为空，在使用浏览器浏览网页时输入要访问的地址即可。



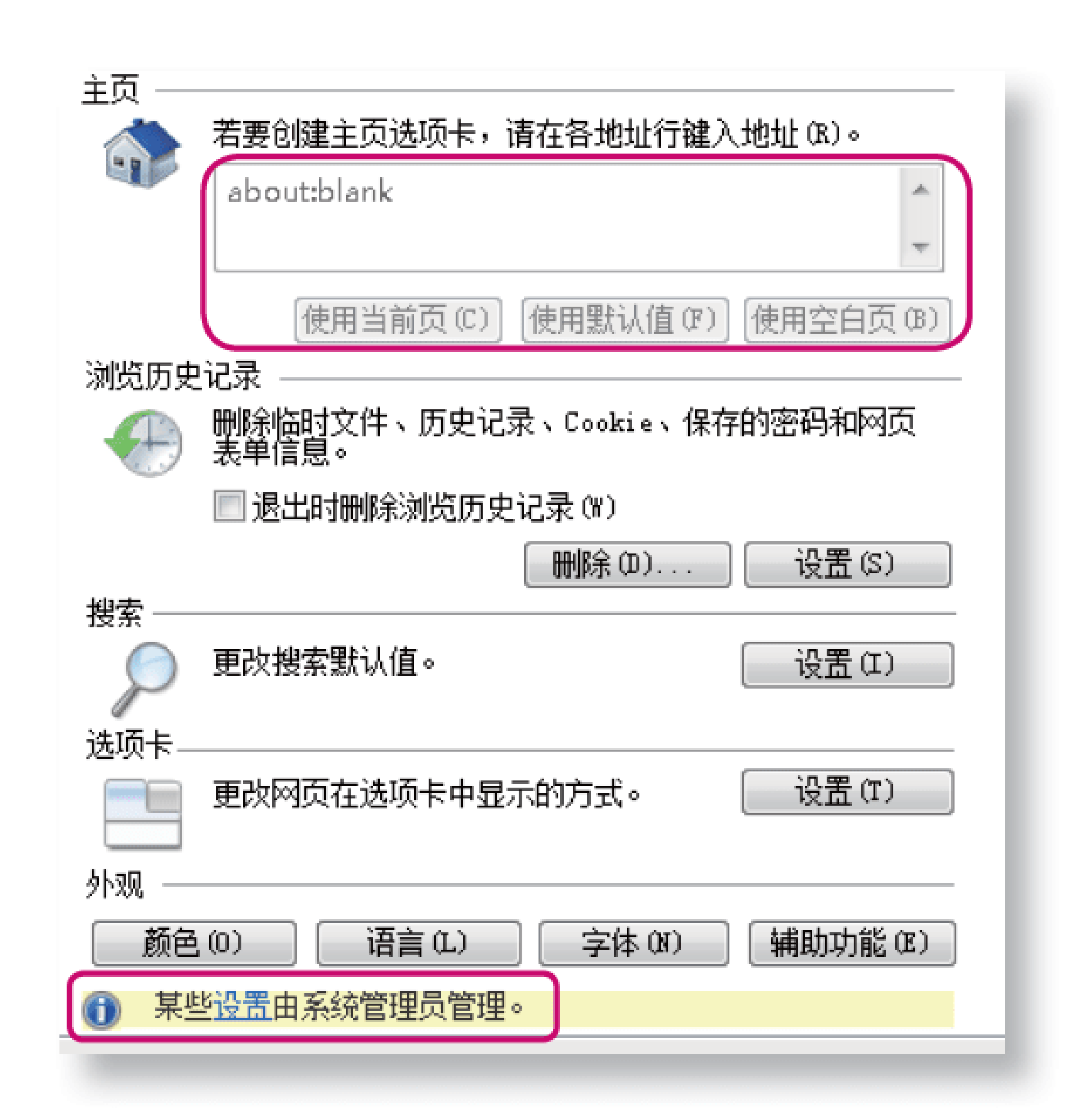
第2步：禁用更改主页

打开注册表编辑器，在左侧窗格中展开HKEY_CURRENT_USER/Software/Policies/Microsoft选项，创建Internet Explorer与Control panel选项，在右侧窗格新建名为HomePage的DWORD值，双击该键值，在打开的对话框中将0修改为1，单击 确定 按钮。

第3步：查看设置效果

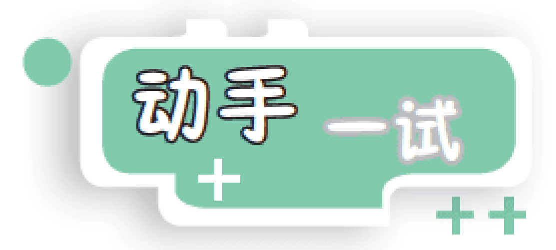
设置完成后，重新打开“Internet选项”对话框，在其中可看到“主页”栏中的设置项目成不可用状态，并在对话框的下方出现“某些设置由系统管理员管理”的提示。

提示：如要恢复设置主页功能，可直接删除或将HomePage的数值数据改为0以实现。



2. 通过组策略禁止

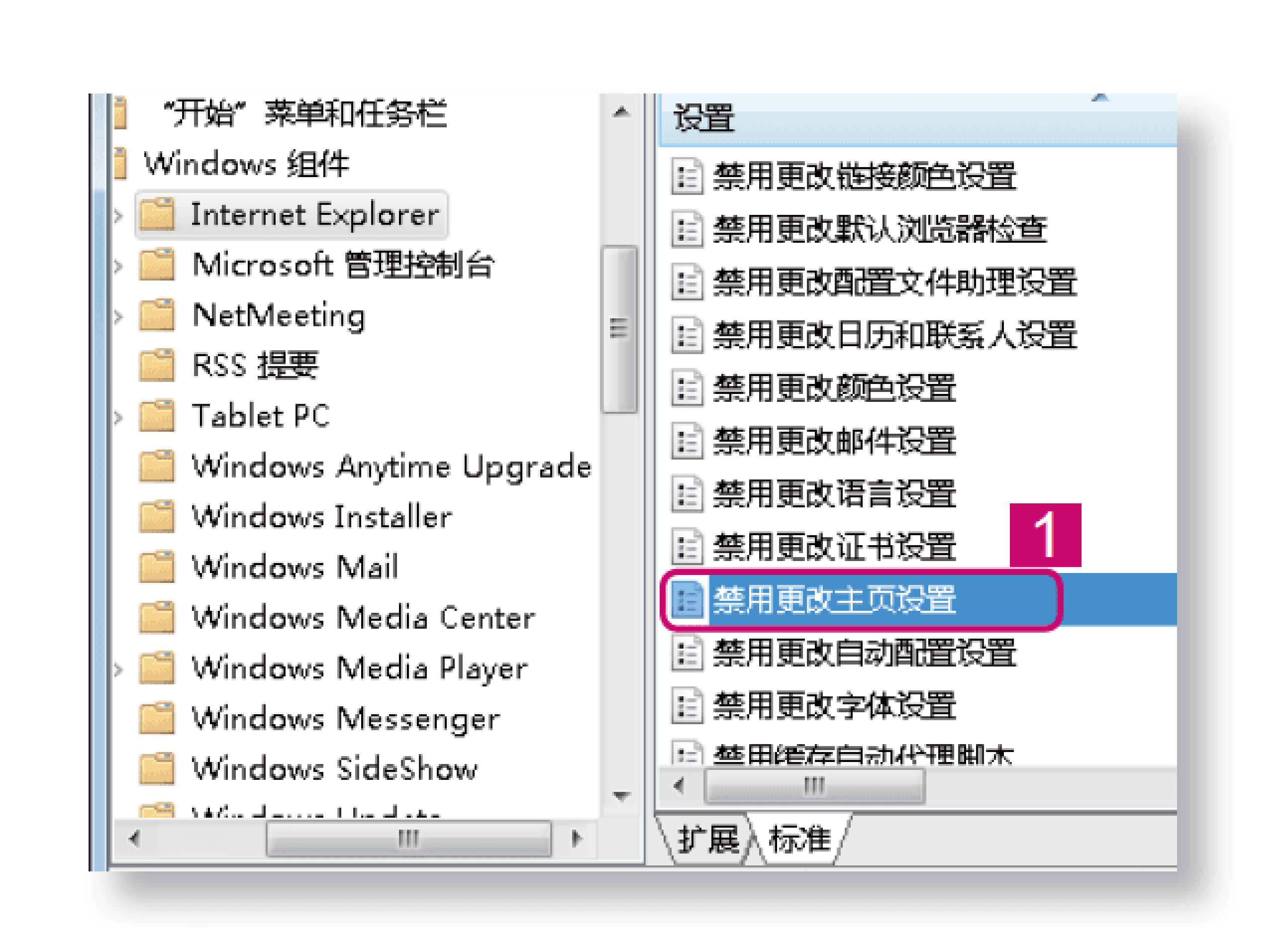
在组策略中设置禁止修改浏览器主页的操作比在注册表中要稍简单，只需选中相应的单选按钮即可。



下面将在组策略中设置禁止更改IE浏览器主页，其具体操作如下。

第1步：展开组策略选项

打开本地组策略编辑器，在其左侧窗格中依次展开“用户配置/管理模板/Windows 组件/Internet Explorer”选项，在右侧窗格中双击“禁用更改主页设置”选项。





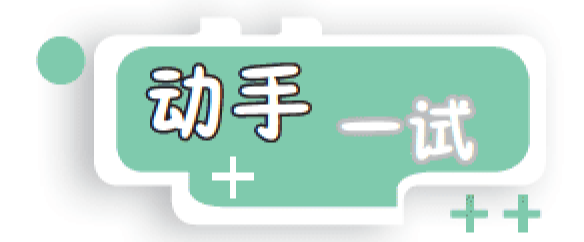
第2步：启用设置

在打开的“禁用更改主页设置”对话框中选中“已启用”单选按钮，然后单击确定按钮应用设置，单击X按钮关闭本地组策略编辑器。

7.2.3 使用360安全卫士清除上网痕迹

使用360安全卫士可对用户上网的浏览痕迹以及一些重要隐私的痕迹进行清理，保证网络中个人信息的安全。





下面将使用360安全卫士清除上网痕迹，其具体操作如下。



第1步：扫描使用痕迹

启动360安全卫士，在打开的主界面中选择“电脑清理”选项卡，然后在其中选择“清理痕迹”选项，在下方可查看到可扫描的对象，单击 开始扫描 按钮即可对上网浏览痕迹、Windows使用痕迹和办公软件使用痕迹等进行扫描。

新手解惑

Q：使用360安全卫士清理痕迹时应注意哪些问题？

A：使用360安全卫士清理电脑使用痕迹时，对于正在使用的程序将自动跳过，因此， 如要彻底清理使用痕迹，扫描前应关闭正在使用的程序。

第2步：清除痕迹

扫描完成后，在界面中将显示扫描的结果，单击 立即清除 按钮，系统将进行清除，清理结束后，将显示清理的总量和所用时间。







在注册表中禁用浏览器的相关选项，并使用360安全卫士清除系统垃圾

任务1：在注册表中的HKEY_CURRENT_USER/Software/Policies/Microsoft/Internet Explorer/Control Panel选项中新建DWORD值SecurityTab和HomePage，隐藏IE安全选项卡并禁止修改主页。

任务2：使用360 安全卫士的电脑清理功能清理系统中的垃圾。

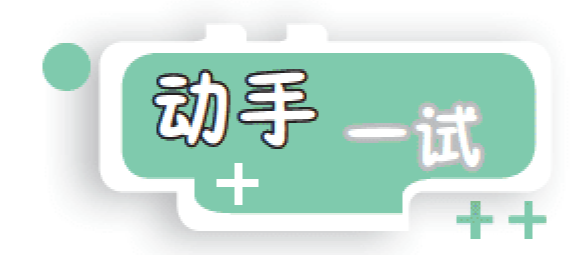


7.3　安全使用电子邮件

最近娜娜的电子邮件常常会收到一些商品的广告和组织的传播文件等垃圾邮件，但是她不知道这些邮件中是否存在安全隐患，就逐个打开。阿伟看见后连忙制止她的这种行为，并且给她讲解怎样安全使用电子邮件。

7.3.1　过滤垃圾邮件

垃圾邮件通常是指未经收件人允许或不知情的情况下，以匿名或伪名的方式，给非法获知的邮箱地址重复发送无意义或乱码的邮件，这些邮件会占用大量的邮箱空间。为了防范垃圾邮件，用户可通过设置过滤垃圾邮件予以杜绝。



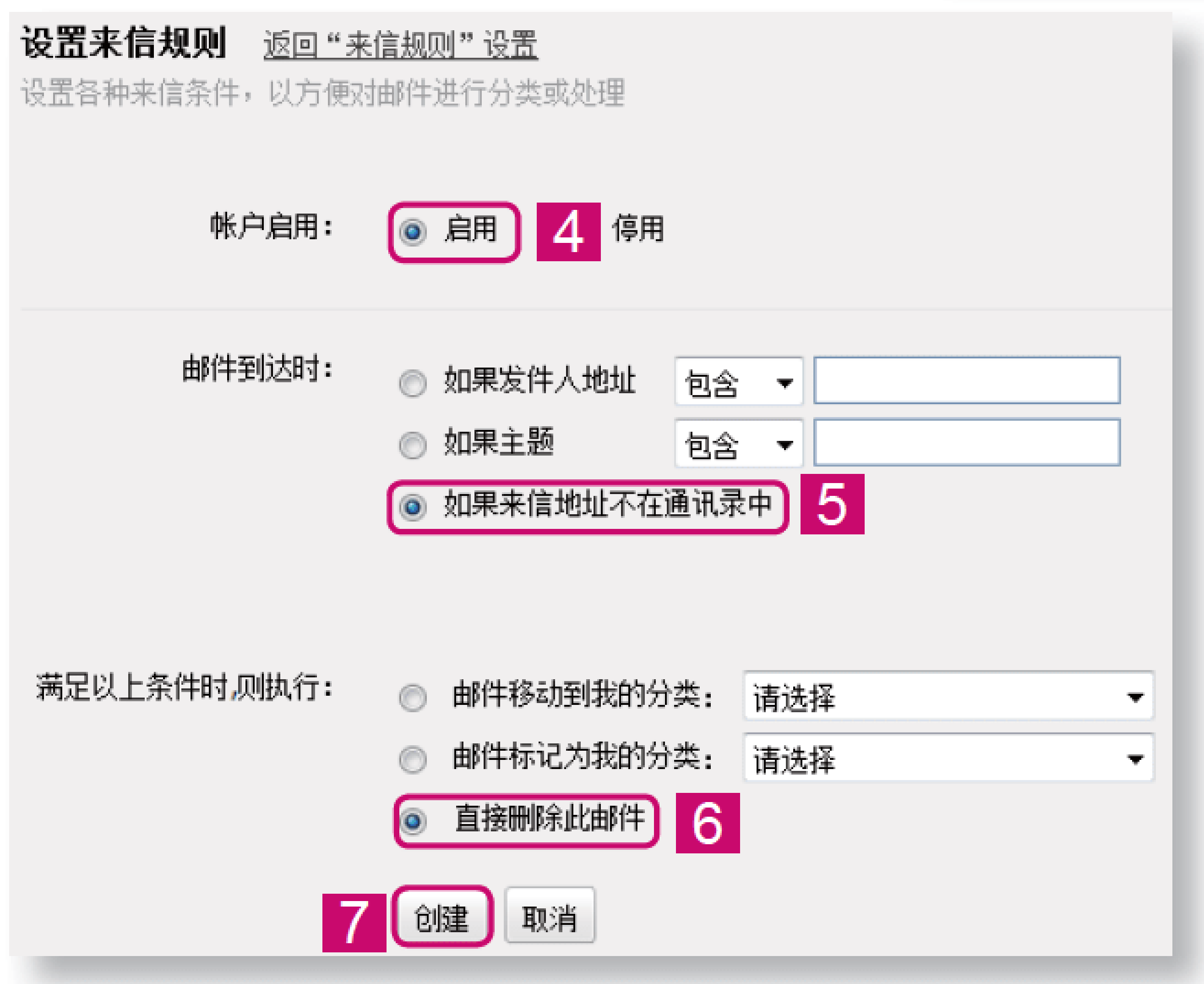
下面以新浪邮箱为例对设置邮箱过滤垃圾邮件进行讲解，其具体操作如下。





第1步：进入设置界面

登录新浪邮箱，在其主界面中单击“设置”超链接，进入设置区，选择“来信规则”选项卡，然后单击 设置来信规则 按钮，进入“设置来信规则”界面。



第2步：设置来信规则

在来信规则设置界面的“账户启用”栏中选中“启用”单选按钮，在“邮件到达时”栏中选中“如果来信地址不在通讯录中”单选按钮，在“满足以上条件时则执行”栏中选中“直接删除此邮件”单选按钮，然后单击 创建 按钮即可。



第3步：查看设置效果

创建规则后，将返回上一级设置页面，在其中将显示创建的来信规则，并可对该规则进行修改或删除操作。

7.3.2 如何防御电子邮件炸弹

电子邮件炸弹攻击不仅会干扰用户正常使用电子邮件，还会影响邮件服务器系统安全，造成整个网络系统全部瘫痪。因此，防御电子邮件炸弹攻击非常重要。



要防御电子邮件炸弹影响用户的正常使用，应考虑以下几个方面。

1．注意网络交流中的行为素质

在网络中不论是在聊天工具还是在论坛上与人辩论，都需注意自身的言辞是否过激或对他人造成名誉攻击，防止对方探查邮箱地址进行攻击，一旦对方知道邮箱地址，便可能对邮箱进行攻击。

不要轻易在论坛上随意张贴网址或产品广告之类的帖子，也不要直接向陌生人的信箱中发送各种有可能被对方认为是垃圾邮件的邮件，因为这样也极有可能引起误会，甚至招致对方的邮件炸弹。

2．谨慎使用自动回信功能

自动回信功能就是指对方给用户邮箱发来一封电子邮件，而用户没有及时收取，邮件系统会按照事先的设定，自动给发信人回复一封确认收到的邮件。这个功能本来是为了方便用户，但很容易被黑客利用，将其制造成邮箱炸弹！如果给你发信的人使用的邮箱账号系统也开启了自动回信功能，那么当你的邮箱收到其发来的邮件而没有及时收取时，系统就会自动向对方发送一封确认信。如果对方在这段时间也没有及时收取信件，又会自动给你发送一封确认收到的信。如此一来，这种自动发送的确认信便会在双方的系统中不断重复发送，直到把双方的邮箱都撑爆为止。

3．设置邮件过滤

为了防范邮件炸弹，很多邮箱服务器都设有过滤功能，该功能可自动过滤包含指定字符的邮件或拒收容量超过设置数值的邮件，将邮件炸弹拒之门外。



跟我练习

设置电子邮件过滤垃圾邮件功能

娜娜的邮箱经常有垃圾邮件，她不知道这些邮件是否带有病毒，因此也不能打开邮件，为了不再收到类似的垃圾邮件，她利用邮箱的过滤功能阻止垃圾邮件的接收。





7.4 安全使用QQ

娜娜有很多朋友需要联系，因此，她经常使用QQ和MSN，但是她知道，使用这些聊天或通信工具不能很好地保证通信的安全性。于是她找到阿伟，想要请教阿伟怎样来做好安全防御。

7.4.1 认识QQ漏洞

如今QQ在国内使用的人数在同类软件中首屈一指，因此这也造成其倍受黑客的“关注”。它除了普通的聊天功能外还扩展了很多方面的业务，如游戏、邮箱以及虚拟货币Q币等。



由于QQ功能的扩展，在无形中就增加了其漏洞存在的可能，为了保护QQ信息不被窃取，需要阻断黑客入侵的途径。常见的QQ漏洞可分为以下几种。

1. 程序漏洞

QQ程序漏洞指该聊天软件本身存在的各种漏洞，黑客可以利用程序漏洞对聊天对象发动信息Flood攻击和IP攻击等，这些攻击为很多用户带来了困扰。他们还利用这些漏洞在使用QQ聊天的过程中散发携带恶意代码的网址和程序脚本等，如臭名昭著的QQ尾巴病毒。

2. 游戏漏洞

QQ游戏中包含了很多休闲和智力游戏，它是腾讯公司随QQ推出的主要软件之一，让人们在工作之余用以放松身心，所以同样拥有大量的用户群体。但它同样也不能逃过黑客的魔掌，通过QQ游戏漏洞刷Q币、刷积分以及窃取QQ号码的行为屡见不鲜，随时都在威胁着用户的利益。





3. 业务漏洞

除了QQ游戏，腾讯公司还推出了QQ Show、QQ空间、QQ邮箱、QQ音乐、QQ直播和QQ宠物等服务，它们都通过Q币支持。因为Q币可以与流通货币相互兑换，这就引起了黑客的觊觎。通过QQ业务漏洞，能非法获得大量Q币、免费对QQ Show和QQ空间进行装饰等。

4. 后台服务漏洞

QQ程序在后台有很多支持服务程序，这也不可避免地会存在漏洞。如TXPlatform.exe进程，它的作用是禁止同一QQ号码多次登录，如果该进程意外中止就可以在一台电脑上登录多个相同号码的QQ，这个漏洞虽然不严重，但是可为用户提升QQ等级。

7.4.2 创建安全的QQ使用环境

用户在使用QQ软件时，可能会遭到病毒的感染或木马的窥探，这不仅会导致个人隐私的泄露，还可能会传播不良的网络信息。因此，创造一个安全的使用环境非常重要。

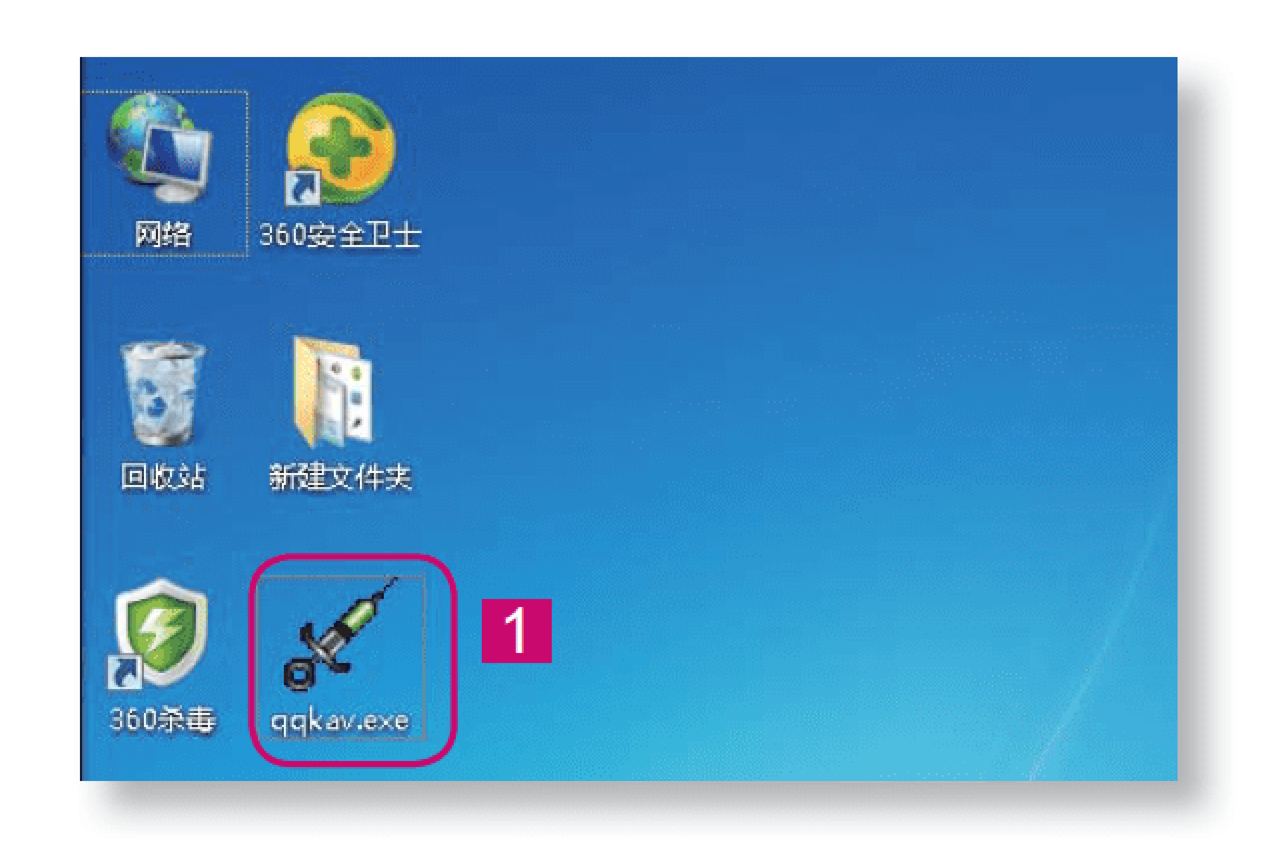
下面将从安装病毒木马专杀工具和提升QQ安全系数两方面进行讲解。

1. 使用QQ病毒木马专杀工具

QQ病毒木马专杀工具是一款专门针对QQ病毒和木马的专杀工具，它具有体积小、病毒库全而且操作简单等优点。使用QQ病毒木马专杀工具可打造一个安全的QQ使用环境。



下面将使用QQ病毒木马专杀工具查杀病毒和木马，其具体操作如下。



第1步：启动QQ病毒专杀木马工具

上网下载该工具（下载地址为http://www.jsing.net/soft/qqkav.exe），解压后双击应用程序将打开QQ病毒专杀工具主界面。

提示：该程序不需安装，双击即可使用，其不占用系统资源。



第2步：查杀病毒

在打开的窗口中单击手动查毒按钮，系统将开始扫描病毒，并显示其扫描进度，完成后在其列表框中将显示扫描到的相关病毒程序的信息。

提示：用户可单击闪电杀毒按钮，系统将扫描病毒并直接将其粉碎。

第3步：粉碎风险程序

在系统扫描出的可疑文件选项上单击鼠标右键，在弹出的快捷菜单中选择“粉碎”命令，系统将对该文件进行粉碎操作，清除该可疑文件。



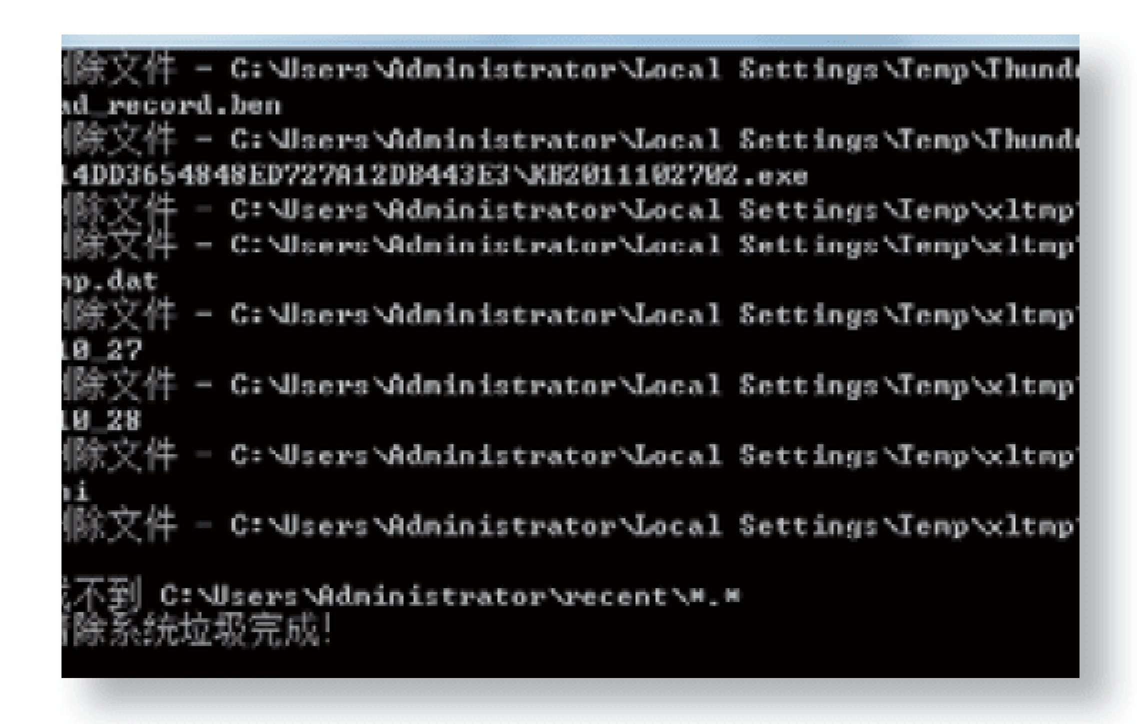
第4步：屏蔽清理

选择“屏蔽清理”选项卡，在其中的“屏蔽功能”栏中选中“启用屏蔽”复选框，在“清理功能”栏中单击立即清理按钮进行垃圾文件的清理。



第5步：清理垃圾文件

系统将打开新窗口，在其中可查看到垃圾文件的清理过程，对于正在使用的相关程序的垃圾清理将不能完成，清理完成后，系统将提示按任意键关闭该窗口。



2. 设置QQ密保

密码保护是腾讯公司开通的一种专门保护QQ账号和密码的服务，用户只需在打开的安全网页上登录QQ号码，然后在其中为QQ设置密码保护，这样即使QQ密码被窃取也可以根据密码保护信息将其找回。



下面将讲解通过申请密码保护提升QQ密码的安全系数，其具体操作如下。



第1步：打开“系统设置”对话框

登录QQ，在其主界面中单击按钮，打开“系统设置”对话框。

提示：也可单击安全按钮，在打开的对话框中选择“我的密保”选项卡，在右侧单击“更多密保手段”超链接，打开“QQ安全中心”网页。

第2步：进入QQ安全中心

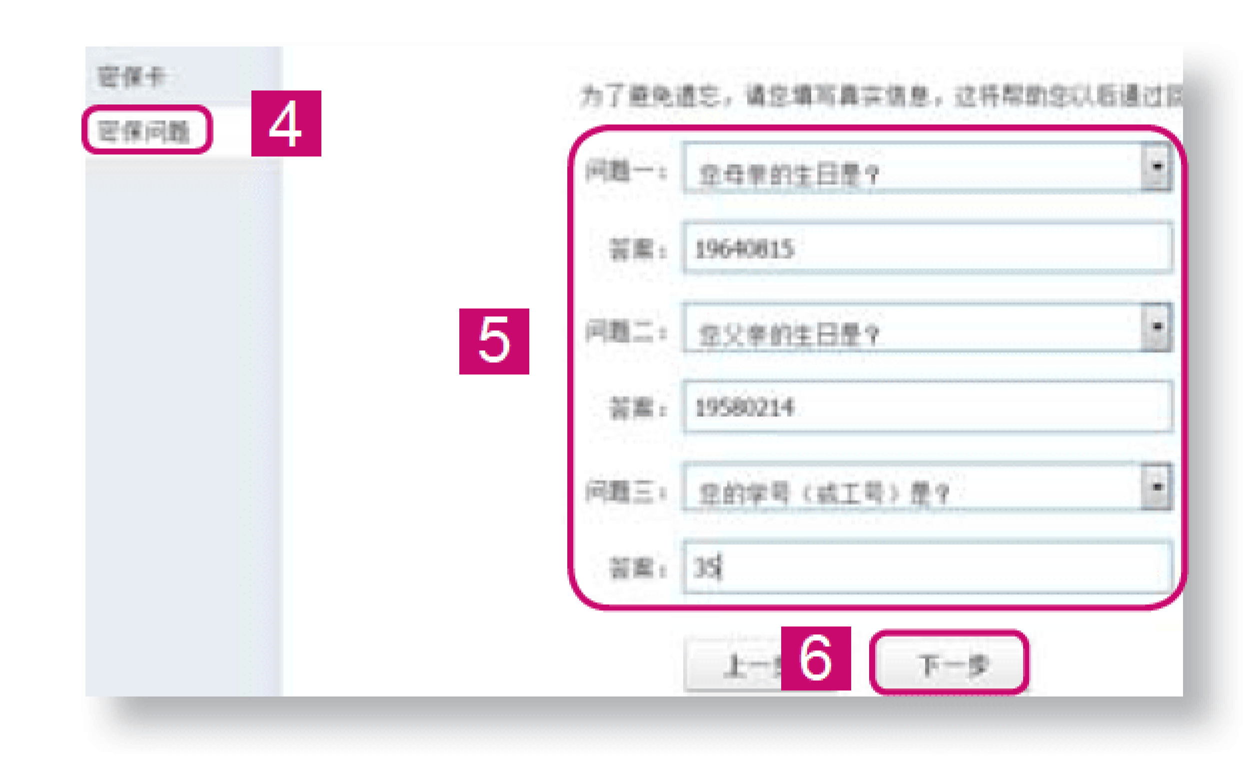
在打开对话框的左侧窗格中选择“安全设置”选项卡，然后在其右侧窗格中单击“申请密码保护”超链接，打开“QQ安全中心”网页。





第3步：设置密保问题

在打开的窗口中选择“密保问题”选项卡，在其右侧的问题下拉列表框中选择要设置的问题选项，在其“答案”文本框中输入问题的答案，然后单击 下一步 按钮。





第4步：验证密保设置成功

在打开的对话框中重新输入设置问题的答案进行验证密保，然后单击 下一步 按钮，在打开的窗口页面中将提示密保设置成功。

跟我练习

为了保证QQ的使用安全，娜娜将使用QQ病毒木马查杀工具对QQ病毒和木马进行查杀，并提升QQ的密码安全

任务1：在网上下载QQ病毒木马工具，然后将其启动，扫描并粉碎电脑中存在的可疑程序。

任务2：为QQ申请密码保护功能以保证其安全性。



7.5 网络安全防御

阿伟告诉娜娜，电脑中的很多不安全因素都是通过网络进行传播的，因此，保障网络的安全性非常重要，网络中的恶意广告和流氓软件等都是影响电脑安全的罪魁祸首。娜娜听了以后问阿伟：“那有什么方法可以防御这些安全隐患呢？”接下来阿伟就开始为娜娜讲解。

7.5.1 阻止恶意网络广告

在浏览网页的过程中，存在一些强迫式的弹出广告，有的会随着鼠标的移动而移动，有的遮挡住了填写电子邮箱地址的边框，有的广告还会播放声音，甚至被黑客利用来攻击用户的电脑，严重影响用户的正常操作。

新手解惑

Q：阻止恶意网络广告有哪些方法？

A：目前使用最广泛的阻止恶意网络广告的软件是360网盾，其具有全面的恶意网络广告阻止功能，且操作简单。另外，遨游浏览器也附带有恶意网络广告阻止功能，用户只需进行简单的设置即可。

1. 使用360网盾拦截广告

360网盾的广告过滤功能可过滤各类浮动窗口广告和弹出广告等，该功能默认是不开启的，可以手动将其开启。



下面将启动360网盾广告过滤功能阻止网络中的恶意广告，其具体操作如下。



第1步：启动360网盾

打开360安全卫士主界面，选择“功能大全”选项卡，然后在“360安全产品”栏中单击“360网”盾按钮，打开360网盾设置窗口。





第2步：开启广告过滤规则

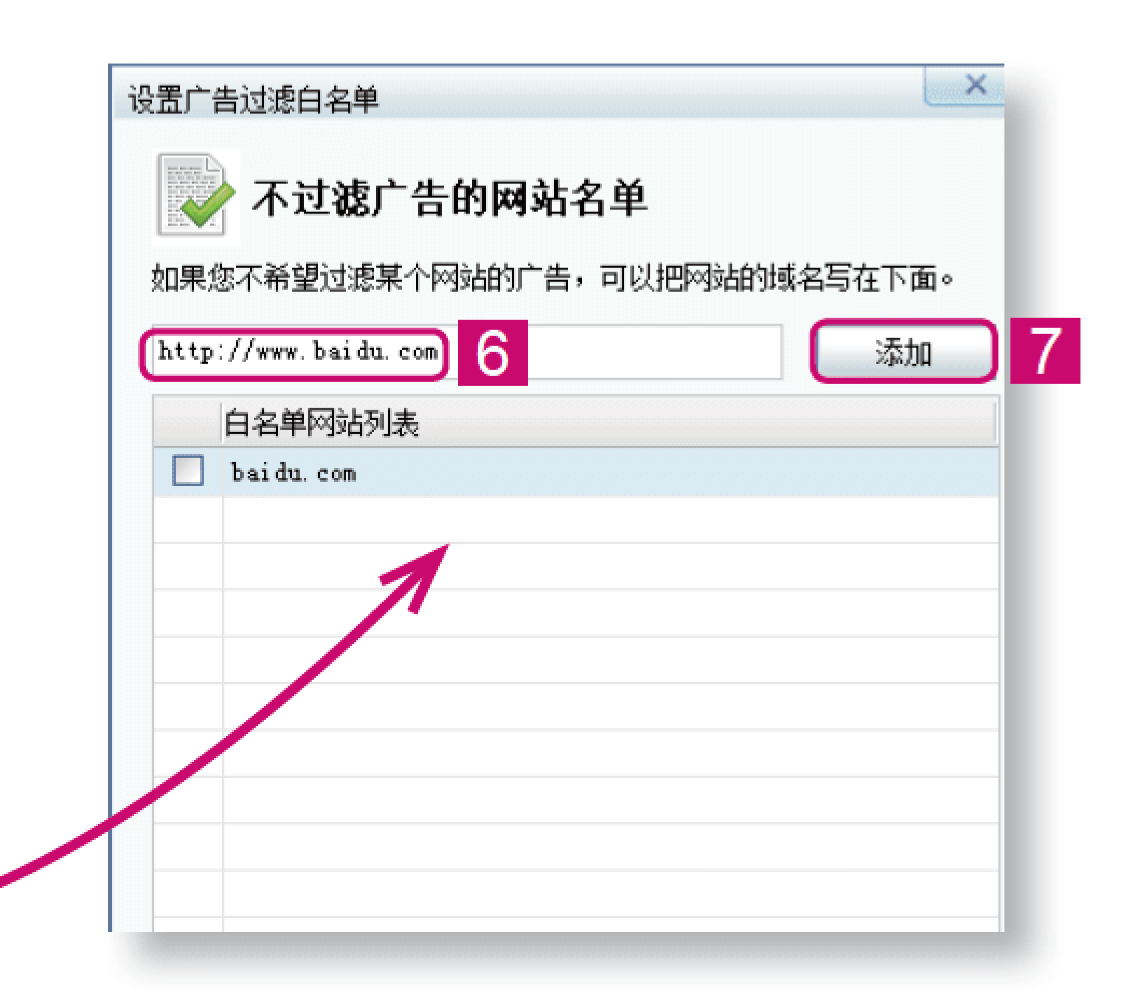
在打开的窗口中选择“广告过滤”选项卡，在其下方单击相应选项的 开启 按钮即可启用相应规则。

提示：在该功能中可过滤网页自动弹出的窗口和漂移广告、浮动广告、Flash广告以及下载站的广告等。

第3步：添加不过滤广告的网站

在“广告过滤”选项卡中单击“不过滤广告的网站”超链接，在打开对话框的文本框中输入不进行广告过滤的地址，这里输入“http://www.baidu.com”，单击 添加 按钮即可。





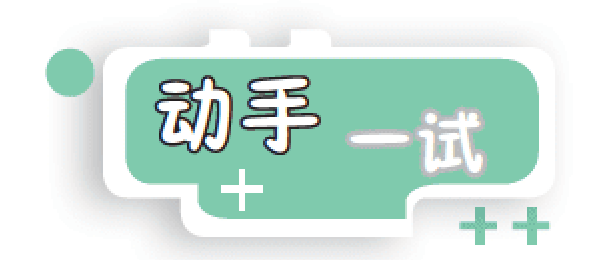
教你一招

显示过滤广告后的提示

在“广告过滤”选项卡中单击“设置”超链接，在打开的窗口中选中“过滤广告后，弹出提示条”复选框即可显示过滤提示。

2. 傲游浏览器的广告拦截功能

傲游浏览器可有效地阻止弹出窗口、各种广告和恶意网页的骚扰，支持自定义过滤和免过滤列表，可方便地添加要过滤的内容。使用傲游浏览器可有效地保障用户上网安全。

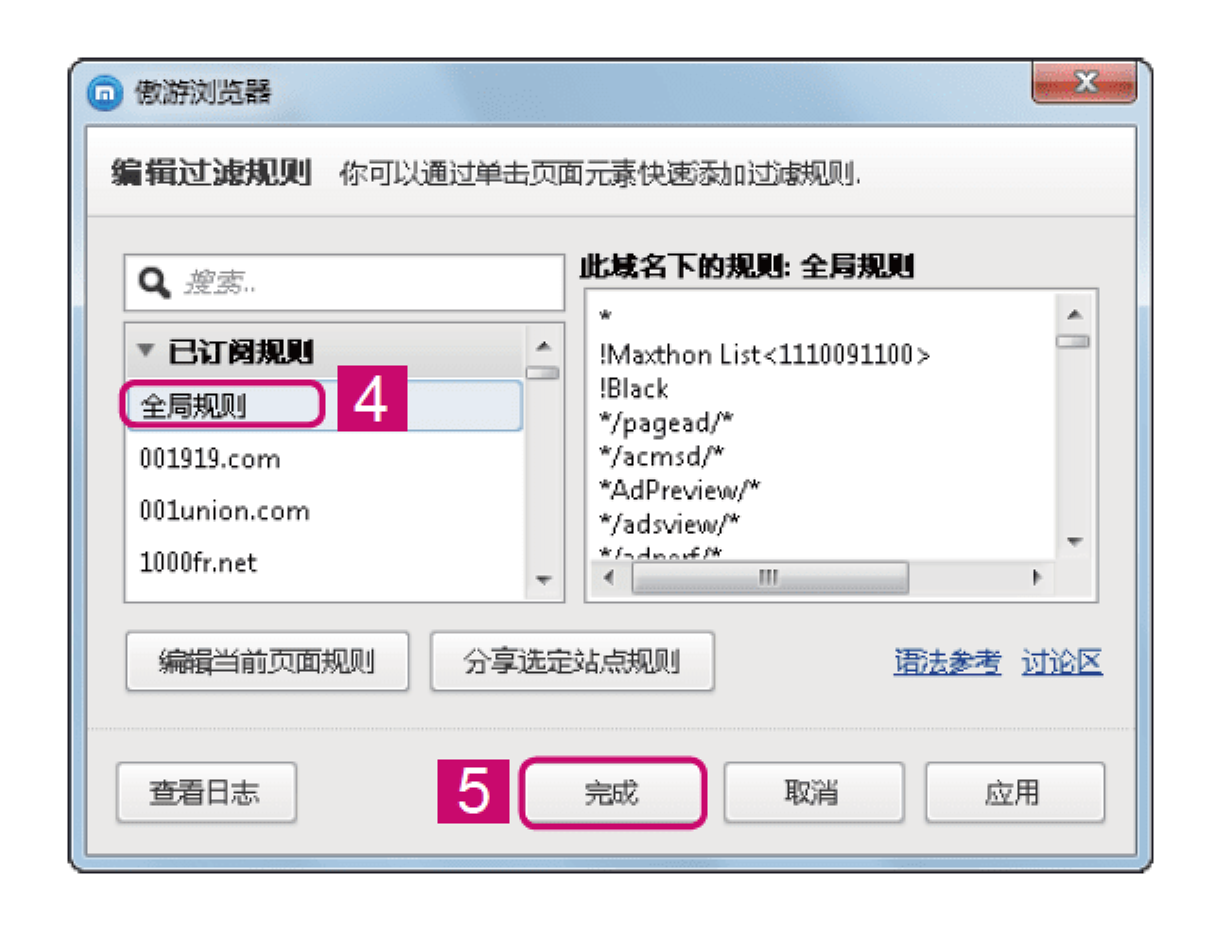


下面将对电脑中安装的傲游浏览器设置广告拦截的方法进行讲解，其具体操作如下。

第1步：启用广告拦截功能

启动傲游浏览器，在其右下方单击按钮，在弹出的菜单中分别选中“启动弹窗拦截”、“过滤本站广告”和“订阅过滤规则”等选项，然后选择“编辑过滤规则”命令。





第2步：编辑过滤规则

在打开的“编辑过滤规则”对话框的“已订阅规则”下拉列表框中选择“全局规则”选项，在其右侧下拉列表框中将显示该规则的具体内容，然后单击按钮即可应用设置的规则。

提示：添加恶意网站广告的网址是一个繁琐的过程，用户最好设置不允许弹出各种广告，再添加一些允许弹出的广告，这样会使操作更简单。

7.5.2 阻止流氓软件入侵

通常，“流氓软件”是指介于病毒和正规软件之间的软件，它们可以采用特殊手段频繁弹出广告窗口，不仅会严重干扰用户的日常工作，而且还会危及数据安全和个人隐私。



1. 流氓软件的分类

所谓的流氓软件，其名称起源于“Badware”一词，是一种跟踪用户上网行为并将用户的个人信息反馈给市场利益集团的软件，并且它们可以通过该软件向用户弹出广告。根据不同的特征和危害，可将流氓软件分为不同的种类。



下面将分别对不同种类的流氓软件进行介绍。

- **广告软件：** 是指未经用户允许，自动下载并安装在用户电脑上，或附加到其他软件上，通过弹出式广告等形式牟取商业利益的程序。此类软件通常会强制安装并无法卸载；在后台收集用户信息牟利，不但危及用户隐私，还频繁弹出广告，消耗系统资源，使系统运行变慢。
- **间谍软件：** 是指那些能够在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。这种软件会使用户的隐私数据和重要信息被后门程序捕获，并发送给黑客、商业公司等。这些后门程序甚至能使用户的电脑被远程操纵，组成庞大的“僵尸网络”，这是目前网络安全的重要隐患之一。
- **浏览器劫持：** 是指一种可通过浏览器插件、BHO（浏览器辅助对象）等形式对用户的浏览器进行篡改的恶意程序，使用户的浏览器配置不正常，被强行引导到商业网站。其危害是用户在浏览网站时会被强行安装此类插件，无法将其卸载，被劫持后，用户只要上网就会被强行引导到其指定的网站，严重影响正常上网浏览。
- **恶意共享软件：** 是指某些共享软件为了获取利益，采用诱骗手段、试用陷阱等方式强迫用户注册，或在软件体内捆绑各类恶意插件，未经允许即将其安装到用户电脑中。其危害是软件集成的插件可能会造成用户浏览器被劫持、隐私被窃取等。
- **行为记录软件：** 是指未经用户许可，窃取并分析用户隐私数据，记录用户电脑使用习惯和网络浏览习惯等个人行为的软件。其危害是危及用户隐私，可能被黑客利用来进行网络诈骗。

教你一招

流氓软件的进化趋势

随着网络的发展，流氓软件的分类也越来越细，一些新种类的流氓软件在不断出现，分类标准必然会随之调整。

2. 防御流氓软件

由于网络发展的速度加快，危害电脑安全的不再只是病毒，流氓软件已经成为最大的危害，用户将不能使用杀毒软件等对其进行彻底清除。



由于杀毒软件并不能清除和防御流氓软件，因此，在防御流氓软件时，应该注意以下几个方面。

- **不随意打开不明网站：** 很多流氓软件都是通过恶意网站进行传播的，一旦用户打开这些恶意网站，操作系统会自动从后台下载这些流氓软件并在用户不知情的情况下安装到电脑中。因此，不要随意打开一些不明网站，特别是一些模仿QQ消息传播的不明网站。
- **尽量到知名网站下载软件：** 流氓软件最广泛使用的传播手段便是与其他正常的软件进行捆绑，在下载信息中通常都会直接播报该软件是否有流氓软件或是其他插件程序。如果播报含有插件或是流氓软件，在下载安装时要多加小心。除了知名的下载网站外，在平时下载软件时，也可以在各软件官方网站直接下载，从官方网站下载的软件含有流氓软件的可能性也较小。当然，在下载软件时，一些不熟悉的软件同样需要注意。
- **安装软件时要仔细：** 很多流氓软件就在单击“下一步”按钮的过程中悄悄安装到了用户的电脑中。在需要选择安装流氓软件时，将相关选项全部取消选中即可避免安装。另外，目前很多软件捆绑了流氓软件后，在安装协议中也会提示用户，但通常在安装软件时，很少有人会耐心地阅读软件安装协议，从而导致严重的后果。
- **不随便安装插件和工具：** 使用绿色的工具代替插件和拦截工具。
- **提高网络安全意识：** 养成良好的上网习惯。用户安装流氓软件很多情况下是由于安全意识低、点击浏览恶意网站等造成的。

教你一招

防御流氓软件的经验总结

安装完操作系统后不要马上上网或插网线，首先应该安装专业杀毒软件和防火墙，并开启流氓软件防御功能。



3. 使用恶意软件清理助手

恶意软件清理助手是一款专用的流氓软件清理工具，其采用全新设计的清理引擎，配合独有的动态分析技术加上不断升级的特征库，以及全新设计的进程管理模块，可以显示隐藏进程，让用户轻易对电脑的运行状态进行掌控。



Q：恶意软件清理助手2011怎么启动？

A：下载了恶意软件清理助手2011后，由于其为绿色软件，可直接双击打开其压缩包，在其中双击rsc2011.exe文件，即可打开恶意软件清理助手2011的主界面。



下面将对使用恶意软件清理助手2011的方法进行讲解，其具体操作如下。



第1步：扫描流氓软件

打开“恶意软件清理助手2011”主界面，选择“恶意软件清理”选项卡，然后在其下方单击“点击此处开始扫描 恶意软件”超链接，系统将自动开始扫描。

第2步：清除流氓软件

扫描完成后，将显示发现的恶意程序，单击“全部选中”超链接选中要清理的软件，然后单击“清理选定项目”超链接，系统将清除恶意软件。



跟我练习

拦截网页广告弹出，清理电脑中的流氓软件

任务1：在360安全卫士中启动360网盾，然后开启恶意广告的拦截功能，使浏览网页时页面更干净。

任务2：在网上下载“恶意软件清理助手2011”程序，扫描并清理电脑中的恶意程序。

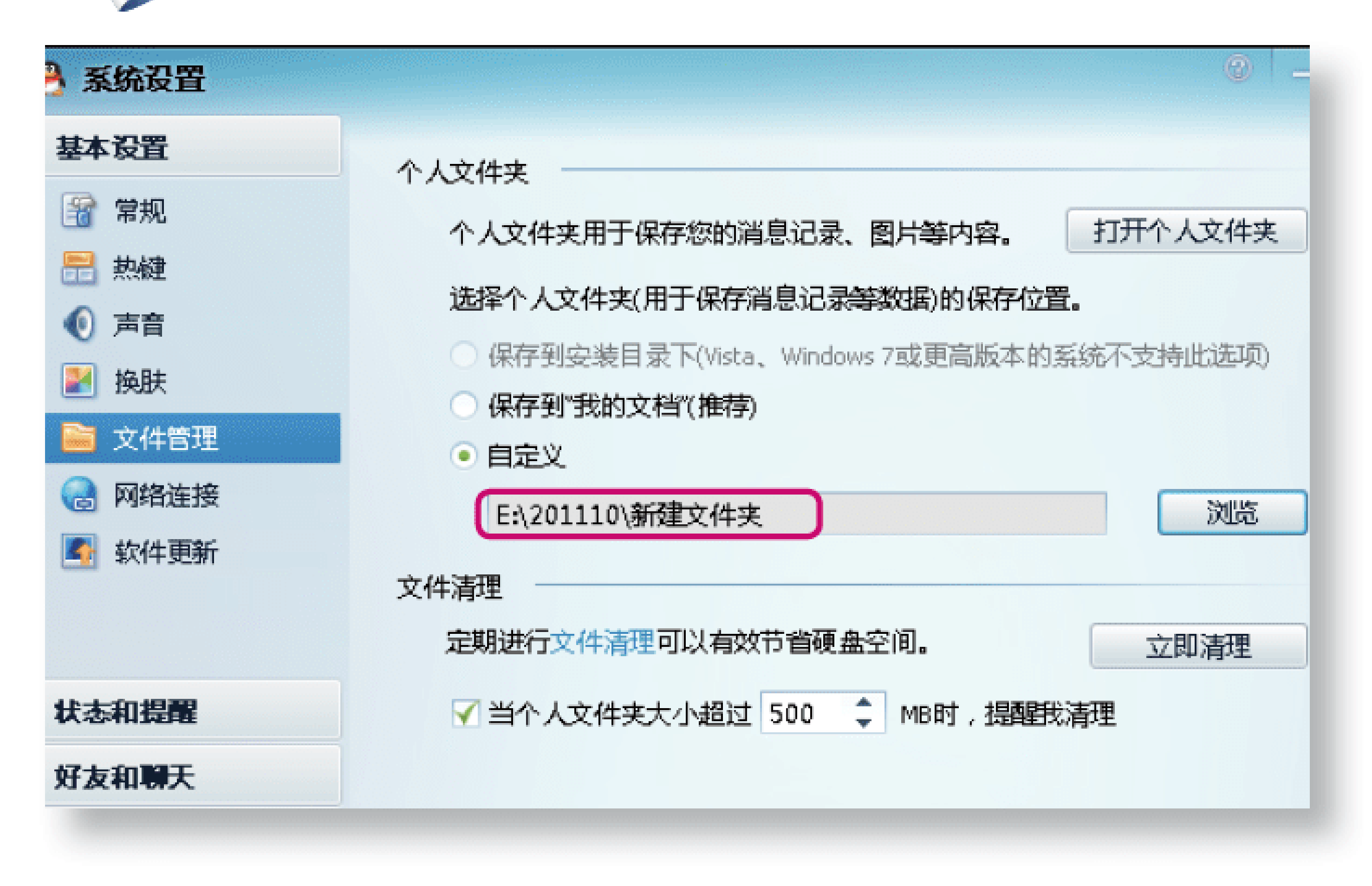
阻止恶意广告弹出

清理恶意程序

7.6 更进一步——轻松保障网络信息安全

为了纠正娜娜平时使用电脑的一些不注意的细节，阿伟打算给娜娜讲解几个需要注意的问题，并且通过实际操作告诉娜娜访问网页和使用聊天软件应注意防止个人隐私的泄露。娜娜听了阿伟的话，想知道自己在哪些方面还做得不足，于是便要求阿伟马上为她讲解。

第1招 备份QQ聊天记录



为了让QQ的聊天记录不被他人窃取，用户还可以将QQ聊天记录的保存位置转移到其他文件夹，并定期进行管理备份，如有必要还可将备份的重要资料进行加密，这样将防止QQ中的重要聊天记录泄露，保证用户能放心地使用QQ，其方法如下：



①启动QQ，打开QQ面板，单击面板左下角的按钮，打开QQ“系统设置”对话框。

②在其左侧窗格中选择“文件管理”选项卡，在其右侧的“个人文件夹”栏中选中“自定义”单选按钮。

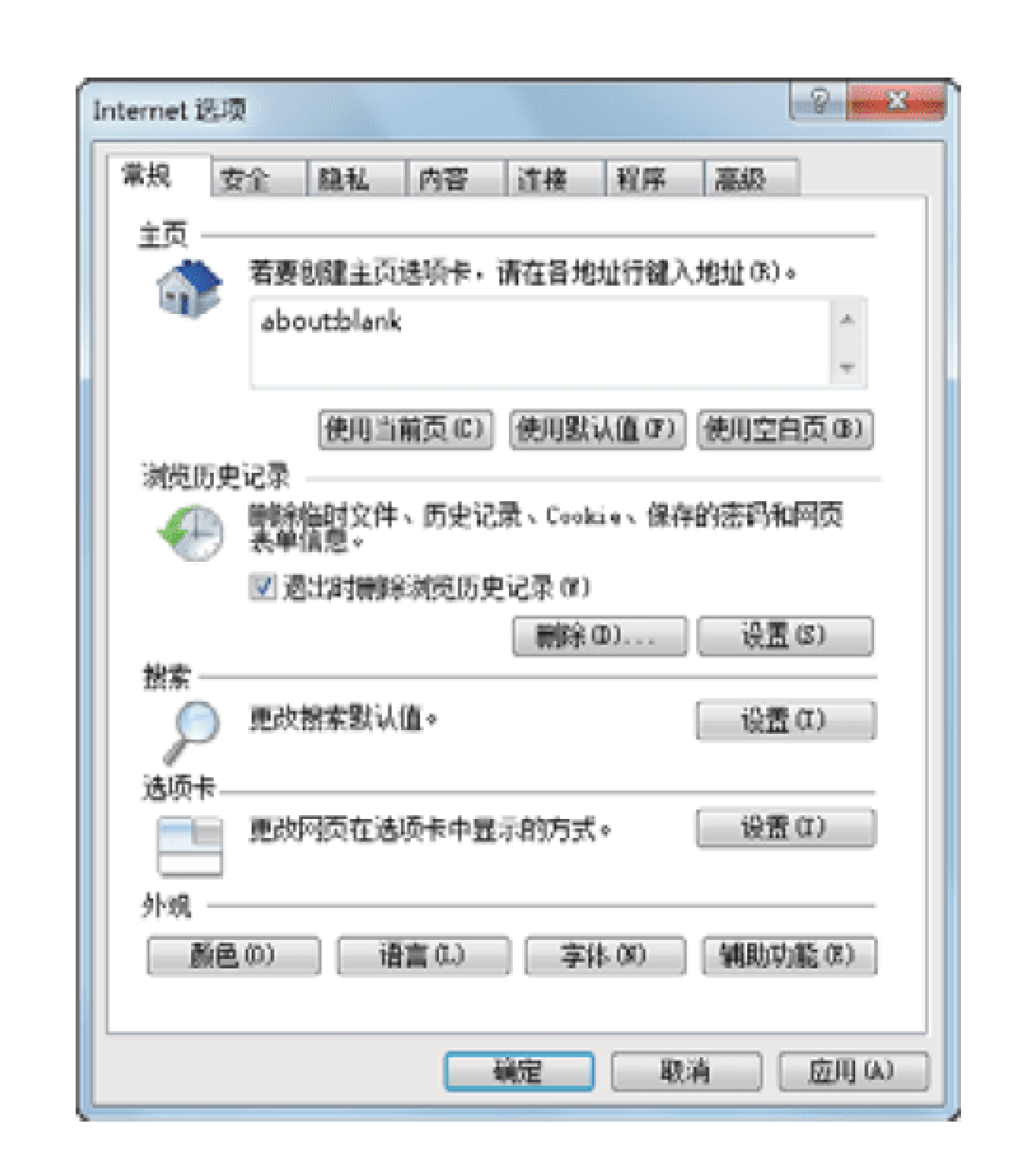
③单击浏览按钮，在打开的对话框中设置保存的路径即可。

第2招 清除IE历史记录

“历史记录”是非常有用的一项功能，但对于公共用户，极容易造成个人信息的泄露，因此，对于这部分用户，可在离开电脑前清除历史记录，其方法如下：

①启动IE浏览器，在其中选择“工具”/“Internet 选项”命令。

②在打开的对话框中选中“退出时删除浏览历史记录”复选框，然后单击确定按钮，即可在每次使用完IE浏览器退出时，将自动清除浏览记录。

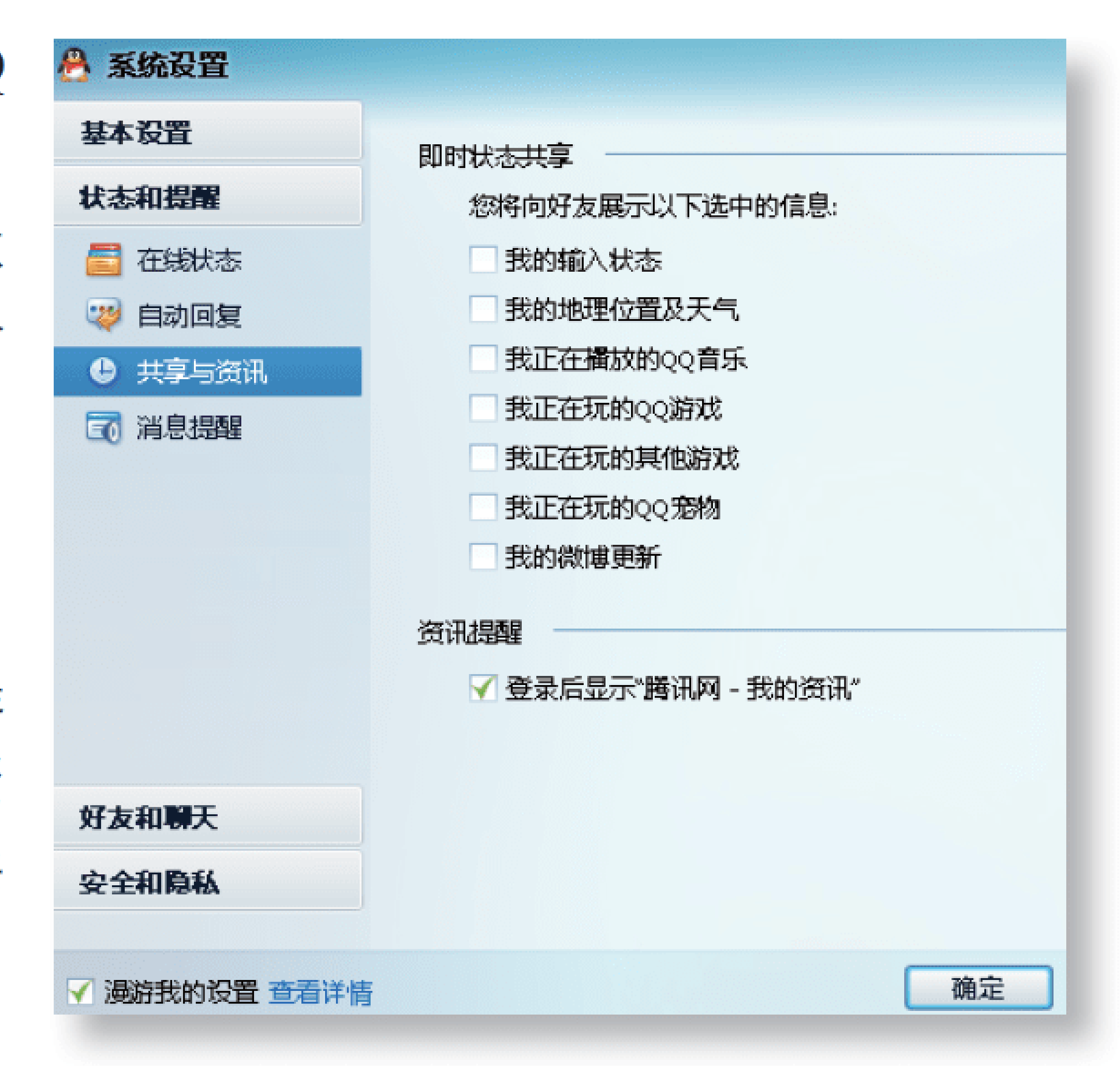


第3招 取消QQ即时状态

在聊天窗口进行文字录入、收听QQ音乐和登录QQ游戏大厅时，别人可在用户的QQ头像下，看到当前用户的即时状态，用户可取消状态的显示，以防止个人隐私泄露，其方法如下：

①启动QQ，单击其面板中的按钮，即可打开“系统设置”对话框。

②在打开的对话框中选择“状态和提醒”选项卡，选择其中的“共享与资讯”选项，在其右侧的“即时状态共享”栏中取消选中相应的复选框。



第4招 监控重要资料的访问行为



使用360隐私保护器可对用户电脑上的重要软件或文件的访问情况进行保护，方便遇到恶意访问时及时进行处理，使用该工具的方法如下：

①启动360安全卫士，在其“功能大全”选项卡中单击“隐私保护器”选项，打开360隐私保护器。

②在打开的窗口中选择“文件访问监测”选项卡，在其中即可设置相应项目进行监控。

7.7　活 学 活 用

（1）打开“Internet 选项”对话框，在其中设置安全级别、可信站点以及阻止弹出窗口和清理历史记录。

（2）通过设置注册表选项禁用“Internet 选项”对话框中的修改主页设置。

（3）进入电子邮件主页中设置过滤垃圾邮件并设置收件规则，以防止垃圾邮件和黑客威胁电子邮件的安全。

（4）登录QQ，为其申请密码保护并安装QQ木马专杀软件和QQ管家，以防止木马对QQ密码的盗取。

（5）简述流氓软件的分类，并上网查询防御流氓软件的方法。



- ☑ 想知道怎样设置密码才能保证其安全性吗？
- ☑ 想知道操作系统中有哪些项目可以设置密码吗？
- ☑ 还在为办公文档的安全性而烦恼吗？
- ☑ 想知道怎样为文件和文件夹设置保护层吗？



第 08 章 给电脑加把锁——加密

今天阿伟打算让娜娜了解电脑中密码设置的一些问题，因为他知道娜娜现在电脑中有很多重要的数据，这些数据没有密码保护是不行的，他提醒过娜娜很多次，让她设置密码，但是娜娜只会一些简单的设置，所以直到现在都还没进行具体的设置。阿伟找到娜娜，对她说："现在给你介绍电脑中一些重要项目的密码设置，你可要认真地学习，学会了以后就不用担心电脑很轻易地遭破坏了。"娜娜认真地点点头，期待着阿伟的讲解。

8.1 密码的安全性

阿伟告诉娜娜："并不是为电脑或文件设置密码后就可以高枕无忧了，我们经常会发现，设置了密码的文件被修改了，其中表现最明显的就是QQ密码经常泄露，因此，密码的安全性非常重要。"娜娜疑惑地问阿伟："那要怎样才能使设置的密码更安全呢？"阿伟接道："这正是接下来要为你讲解的知识！"

8.1.1 提高密码的安全性

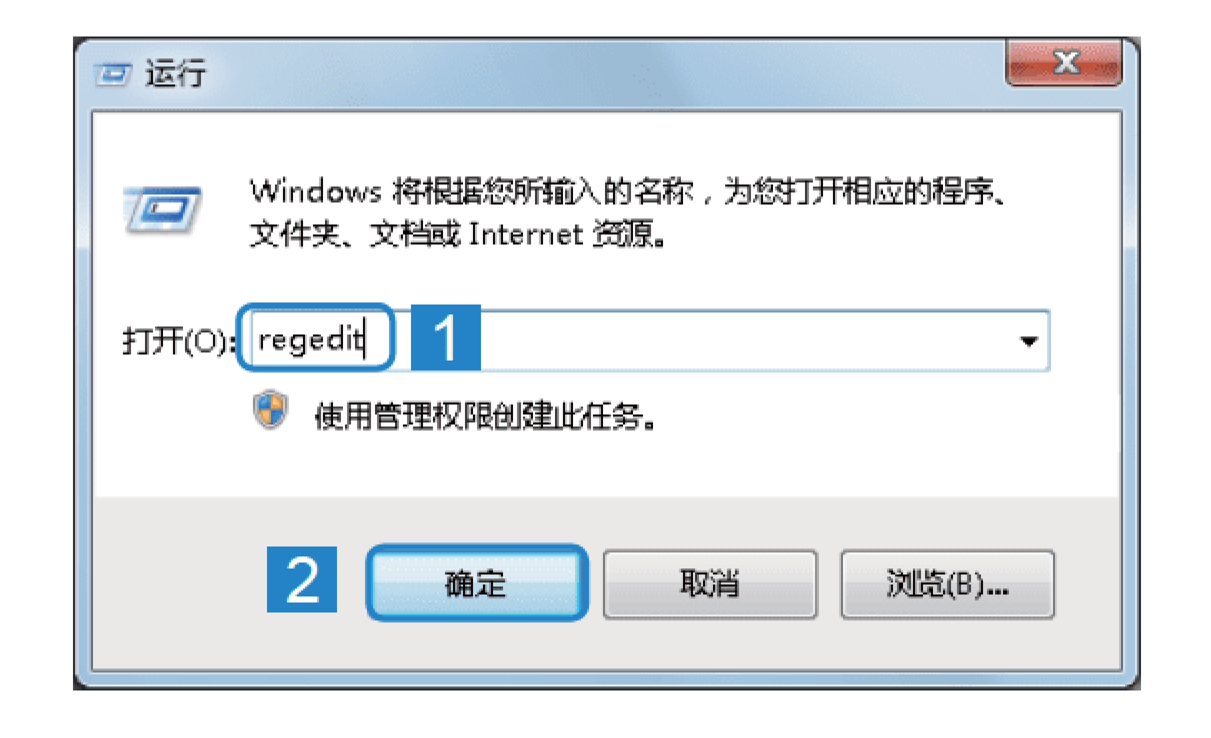
很多时候，人们设置密码的方法都是不够安全的，为了使设置的密码能保障设置对象的安全，通常可通过对注册表和组策略的设置来提高密码的安全性，下面将对其分别介绍。

1. 使用注册表限制密码格式

在实际应用中，用户可通过限制密码格式来达到设置安全密码的目的。限制密码格式是指在注册表中进行设置，使用户使用的密码不能为空，只能是字母、数字或字母和数字的组合。



下面将对在注册表中新建键值项设置限制密码的格式的方法进行讲解，其具体操作如下。

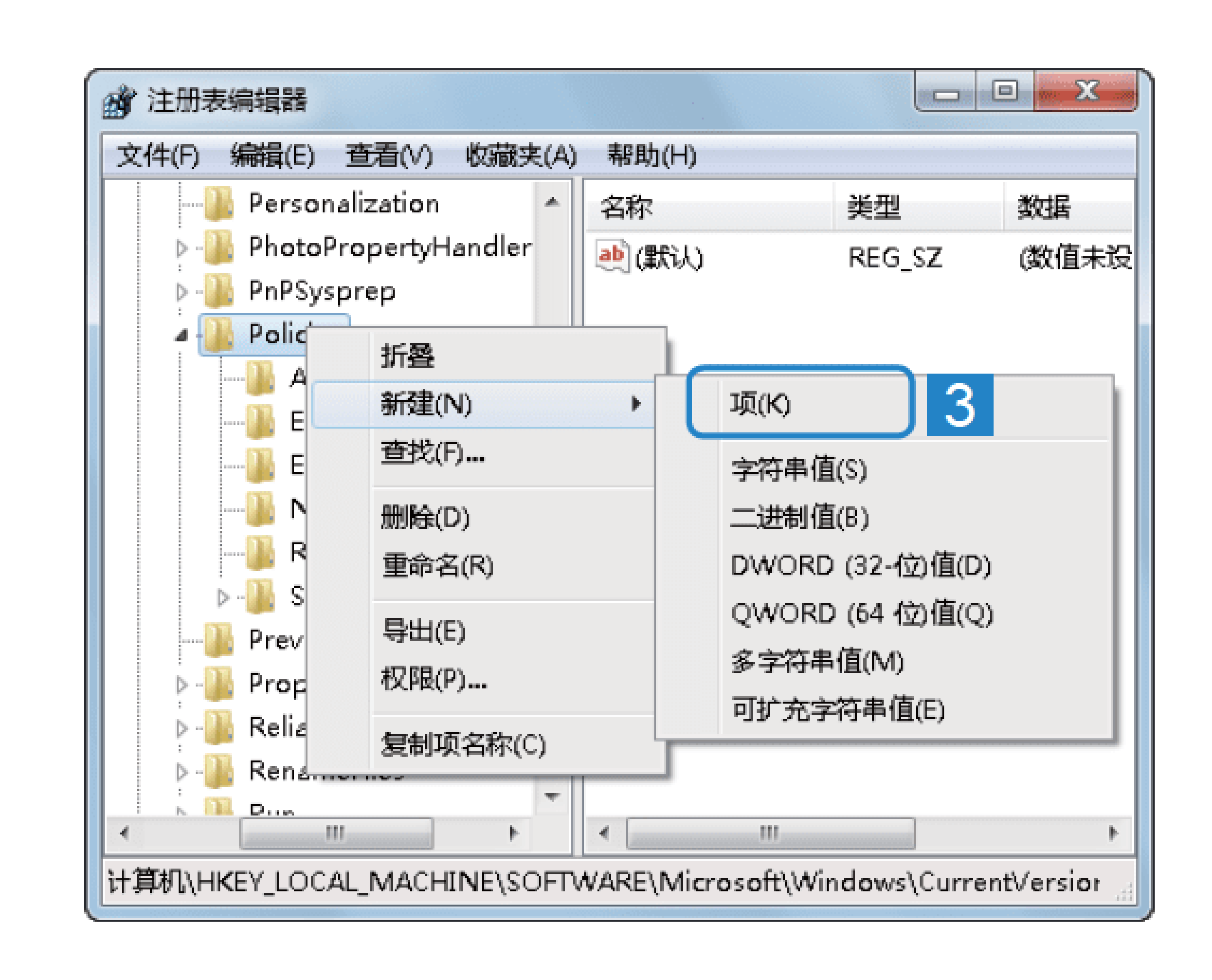


第1步：打开注册表编辑器

选择"开始"/"运行"命令，打开"运行"对话框，在"打开"文本框中输入"regedit"，然后单击 确定 按钮，打开注册表编辑器。

提示：对注册表进行修改时一定要小心，一旦出现错误，很容易导致系统崩溃，所以最好不要轻易动手修改注册表。





第2步：新建项

在打开的注册表编辑器中展开HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Policies选项，在Policies选项上单击鼠标右键，在弹出的快捷菜单中选择“新建”/“项”命令，将新建的项命名为Network。

第3步：新建DWORD值

在右侧窗格中单击鼠标右键，在弹出的快捷菜单中选择“新建”/“DWORD（32位）值”命令，将新建的DWORD值命名为AlphanumPwds，双击该键值，在打开的对话框中选中“十六进制”单选按钮，在“数值数据”文本框中输入“1”，单击确定按钮完成设置。

2. 使用组策略加强密码安全

用户可在组策略中进行设置，避免习惯性地输入不安全的密码，达到强制要求密码必须具有一定复杂性的目的。

新手解惑

Q：在组策略中可设置哪些选项来加强密码的安全性？

A：在组策略中可通过限制密码长度，设置密码的最长存留期，以强制定期更换密码；还可以设置强制密码历史，以使多次设置的密码不重复。

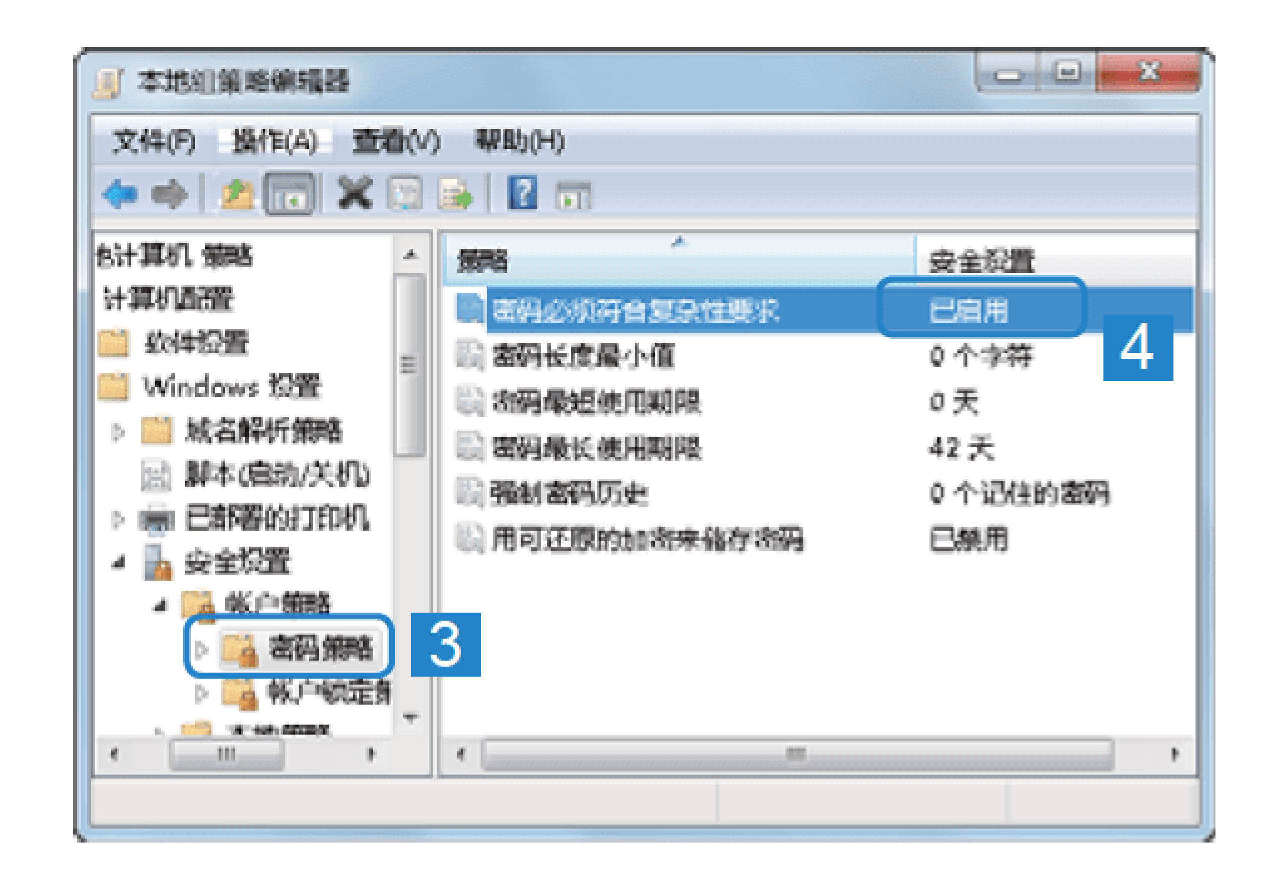


下面将对在组策略中通过设置相关选项以加强密码的安全性的方法进行讲解，其具体操作如下。



第1步：打开组策略编辑器

选择“开始”/“运行”命令，打开“运行”对话框，在“打开”文本框中输入“gpedit.msc”，然后单击 确定 按钮打开本地组策略编辑器。



第2步：启用密码的复杂性要求策略

在本地组策略编辑器的左侧窗格中展开“计算机配置/Windows设置/安全设置/账户策略/密码策略”选项，在右侧窗格中双击“密码必须符合复杂性要求”选项，在打开的对话框中选中“已启用”单选按钮，单击 确定 按钮。

第3步：设置密码长度最小值

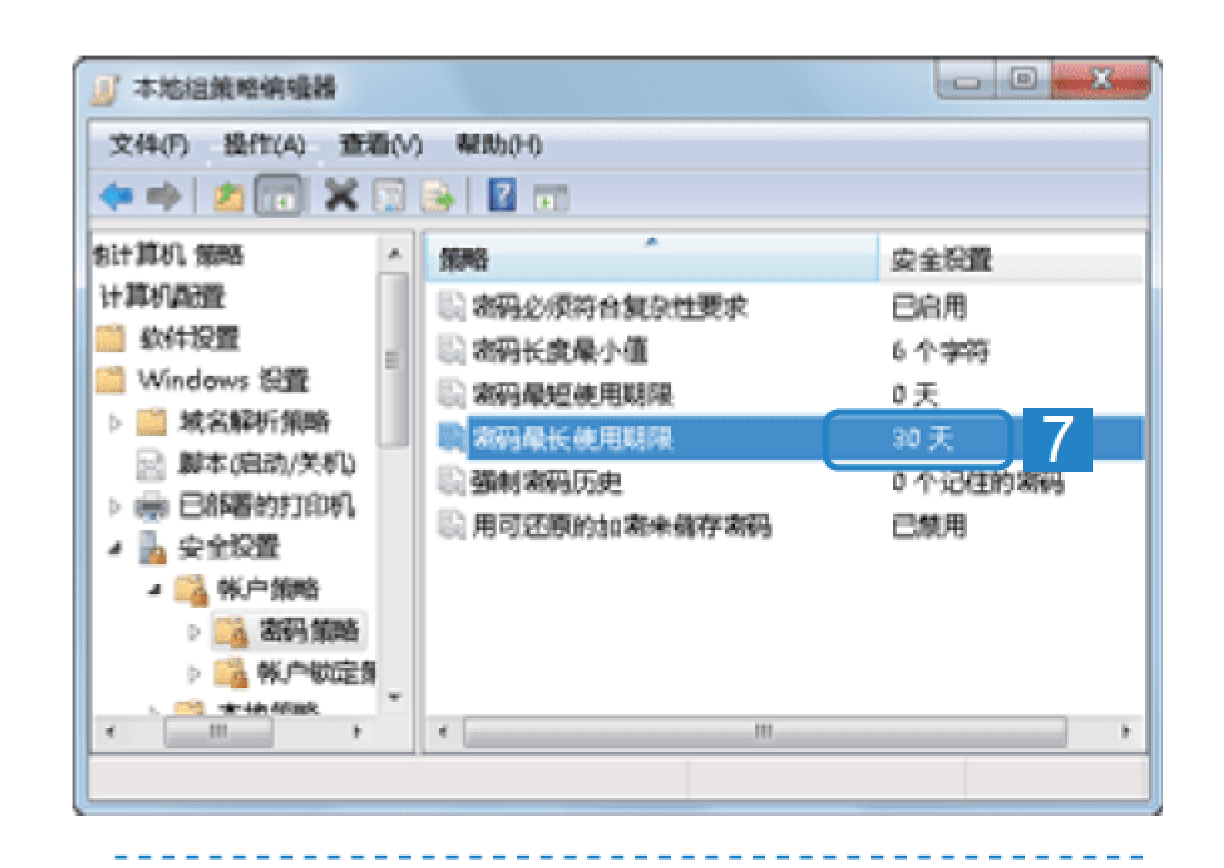
在返回的组策略窗口中双击“密码长度最小值”选项，打开“密码长度最小值 属性”对话框，在“密码必须至少是”数值框中输入密码的最小输入长度，这里输入“6”，单击 确定 按钮应用设置。





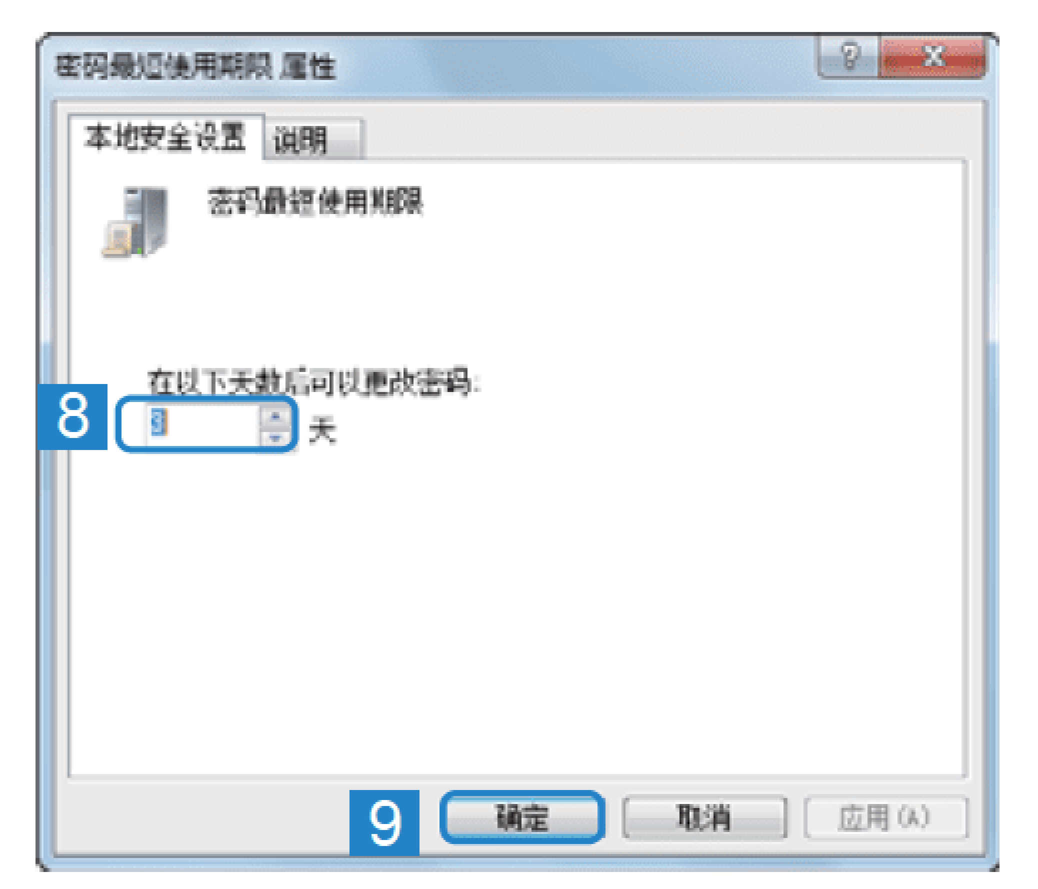
第4步：设置密码最长使用期限

双击“密码最长使用期限”选项，打开“密码最长使用期限 属性”对话框，在“密码过期时间”数值框中输入密码过期的天数，这里输入“30”，单击确定按钮。



第5步：设置密码最短使用期限

双击“密码最短使用期限”选项，打开“密码最短使用期限 属性”对话框，在“在以下天数后可以更改密码”数值框中输入密码最短存留的天数，这里输入“3”，单击确定按钮。



第6步：设置强制密码历史

双击“强制密码历史”选项，打开“强制密码历史 属性”对话框，在“不保留密码历史”数值框中输入保留密码历史的个数，这里输入“1”，单击确定按钮。最后关闭编辑器窗口完成设置。

8.1.2 保护密码安全的措施

很多用户在平常对密码的设置不注重，因此给网络和电脑带来了非常严重的安全隐患。为了使密码的安全性得到保证，在平常使用时应注意使用的相关原则。



下面介绍几种提高密码安全性的方法。

- **设置长密码：**8位以上的数字、字母和符号组合而成的密码使用暴力破解是要花费很长时间的，使用生僻的符号还能让黑客字典毫无用处。
- **尽量不使用相同的账号密码：**用户为了记忆方便，在登录邮箱、论坛或其他社区都使用相同的账号和密码，这样是非常危险的，因为一旦某个密码被破解，那就意味着所有的账号和密码都有被破解的可能。
- **不使用容易得到的信息作为密码：**这里所指的信息包括电话号码、手机号码和身份证号码等。
- **不随便透露密码信息：**不要将自己的密码信息随便透露给别人，尤其是网上一些所谓的朋友。
- **申请密码保护：**申请密码保护可以为ID和密码提供多一层的保障，如果密码丢失，可以根据有效资料将其找回。
- **定期清除木马：**一旦电脑中了木马，它会通过键盘记录和截屏等方式记录密码并将其发送给黑客，不仅如此，电脑中的各种信息都岌岌可危。

8.1.3 常见密码泄露的现象

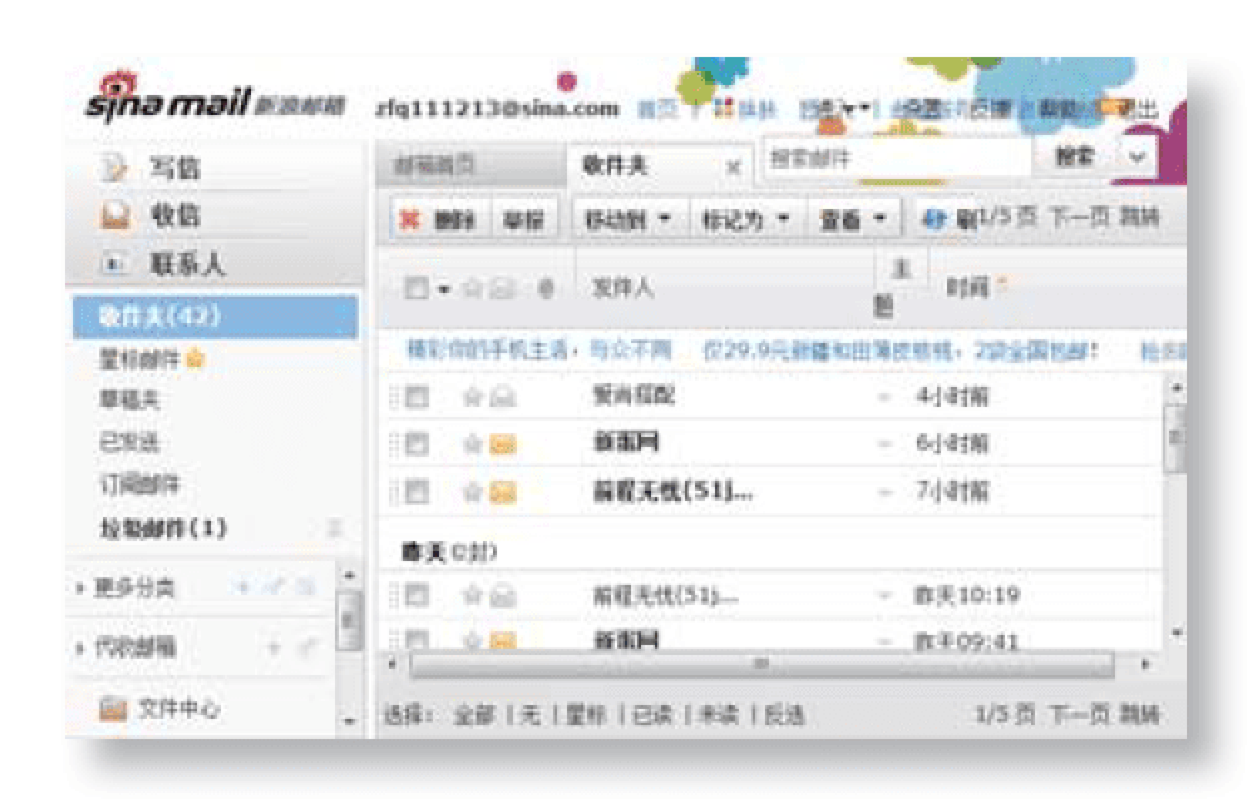
在日常生活中，用户经常会遇到自己的重要密码泄露的现象，这些情况给用户的财产安全和个人隐私带来了极大的威胁，使用户苦不堪言，如邮件密码的泄露、办公文件及文件和文件夹等。可见，密码的安全性对用户是多么的重要。



下面将对这几种现象造成的危害进行介绍，主要包括以下几种情况。

1. 邮箱密码泄露带来的后果

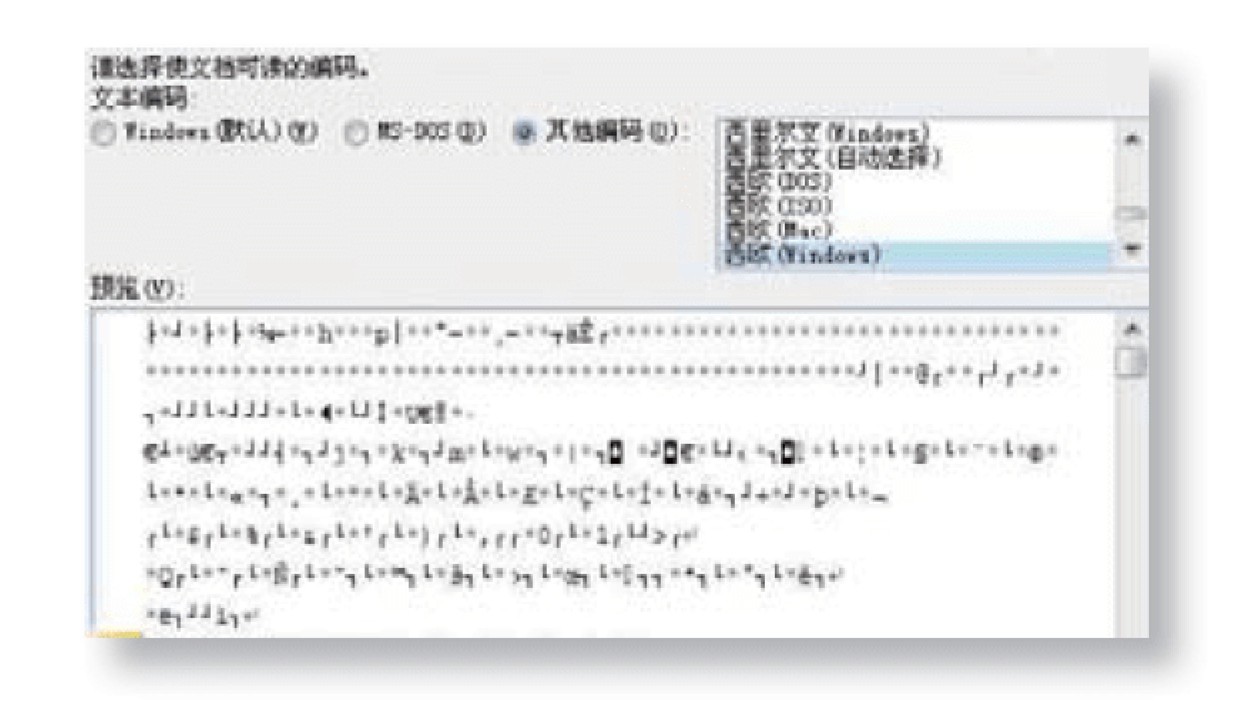
如果用户邮箱密码泄露，会被一些不法分子利用该邮箱收发用户重要的邮件，将造成用户钱财的损失或对他人造成困扰。除此之外，由于不法人员违法使用邮箱，造成邮箱中大量垃圾邮件的产生，或被他人使用邮箱炸弹进行攻击，造成邮箱无法使用的情况。





2. 办公文件被恶意访问

如果用户的电脑中有重要的办公文档未对其进行加密，这就给他人获取电脑的重要信息提供了方便，通常对办公文档的破坏包括修改其中的内容，或将文件损坏，因此，用户应养成为重要办公文档进行加密的习惯。





3. 文件或文件夹被损坏

电脑中有很多文件和文件夹，通常这些文件和文件夹都没有任何的权限设置，用户可以任意访问，但对于重要的文件或文件夹，如遭到破坏，将使用户造成很大的损失，因此，为文件和文件夹加密也非常必要。

跟我练习

限制密码的格式并通过组策略设置密码的安全性

任务1：打开注册表编辑器，在其中添加相应的键值，限制其密码的输入形式为字母和数字。

任务2：打开组策略编辑器，在其中设置密码的最小长度为8，最长使用期限为“7天”。

注册表

组策略

8.2　操作系统加密

阿伟告诉娜娜，为操作系统加密可对系统的登录密码、屏幕保护密码和电源管理密码进行设置，这样可在多方面对系统进行保护。娜娜心想：“以前自己就知道系统的登录密码的设置，对于阿伟所说的都没有听过，现在一定要好好地让阿伟为自己讲解一下。”



Q：怎样的密码才是安全的密码？

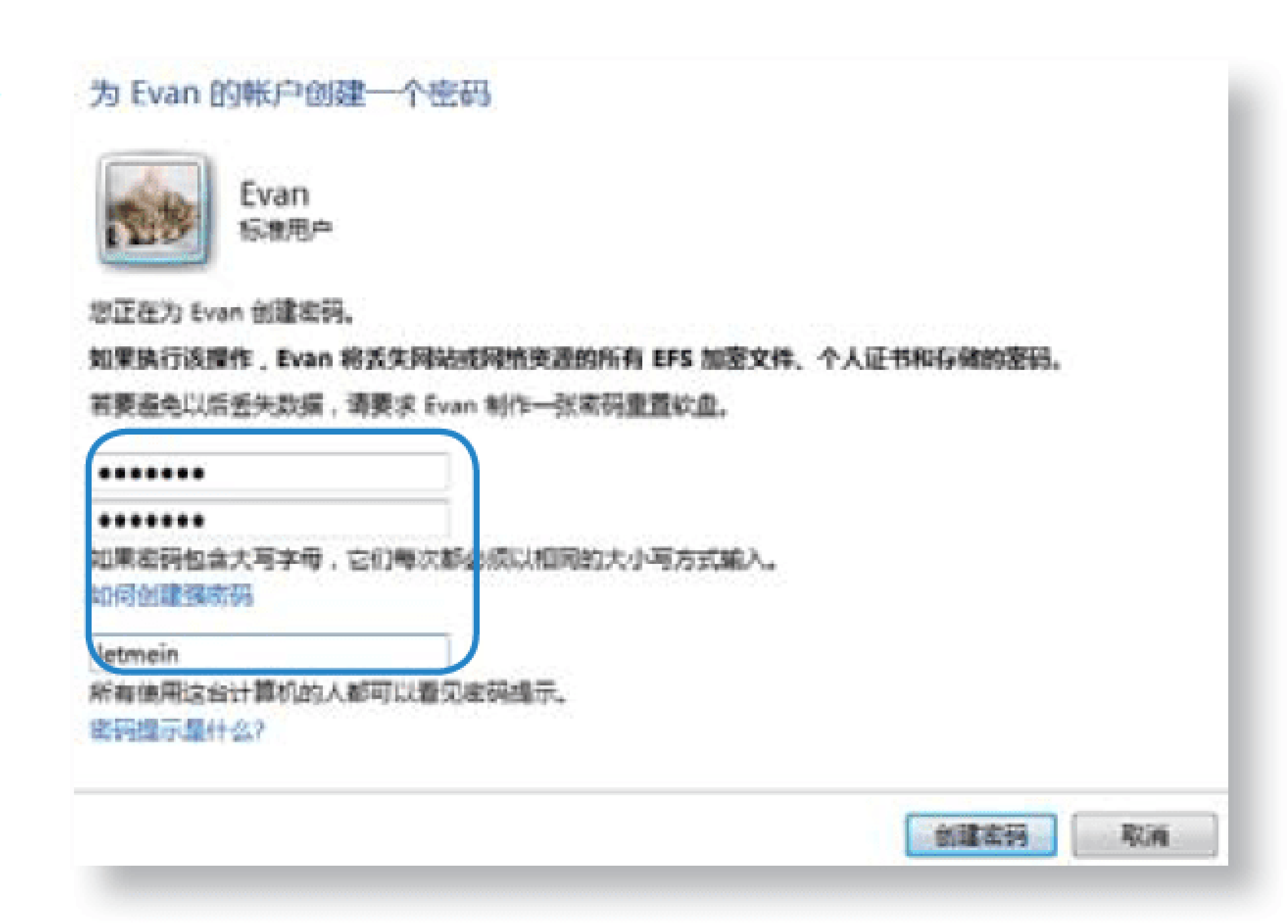
A：将密码设置为8位数以上的字母、数字和其他符号的组合，同时加入其他特殊符号，如“#”、“*”或“&”等。密码要同时包含拼音和数字，最好不要用完整的英文单词或其他对应汉语拼音，可将其顺序打乱。不重复使用同一密码。

8.2.1　设置登录密码

登录密码为用户的电脑提供了一种安全保护，可以避免他人使用电脑，从而保障电脑和重要数据的安全，其具体是指使用某个账户登录到操作系统时所使用到的密码。

要保护操作系统的安全，最直接且最简单的方法就是设置用户账户的密码，这样就能防止他人进入操作系统，对其进行修改。

提示：前面已经介绍过为用户账户设置密码的方法，这里不再赘述。



8.2.2　设置屏幕保护密码

如果用户想暂时离开电脑，但又不希望其他用户查看自己电脑中的信息，可启动设置了密码的屏幕保护程序，从而阻止未授权用户访问电脑。屏幕保护程序简称屏保，它是一个可以使屏幕暂停显示或以动画的方式显示的应用程序。





下面将对设置屏幕保护密码的方法进行讲解，其具体操作如下。



第1步：启动屏幕保护程序设置

在桌面空白处单击鼠标右键，在弹出的快捷菜单中选择“个性化”命令，然后在打开的窗口中单击“屏幕保护程序”超链接，系统将打开“屏幕保护程序设置”对话框。



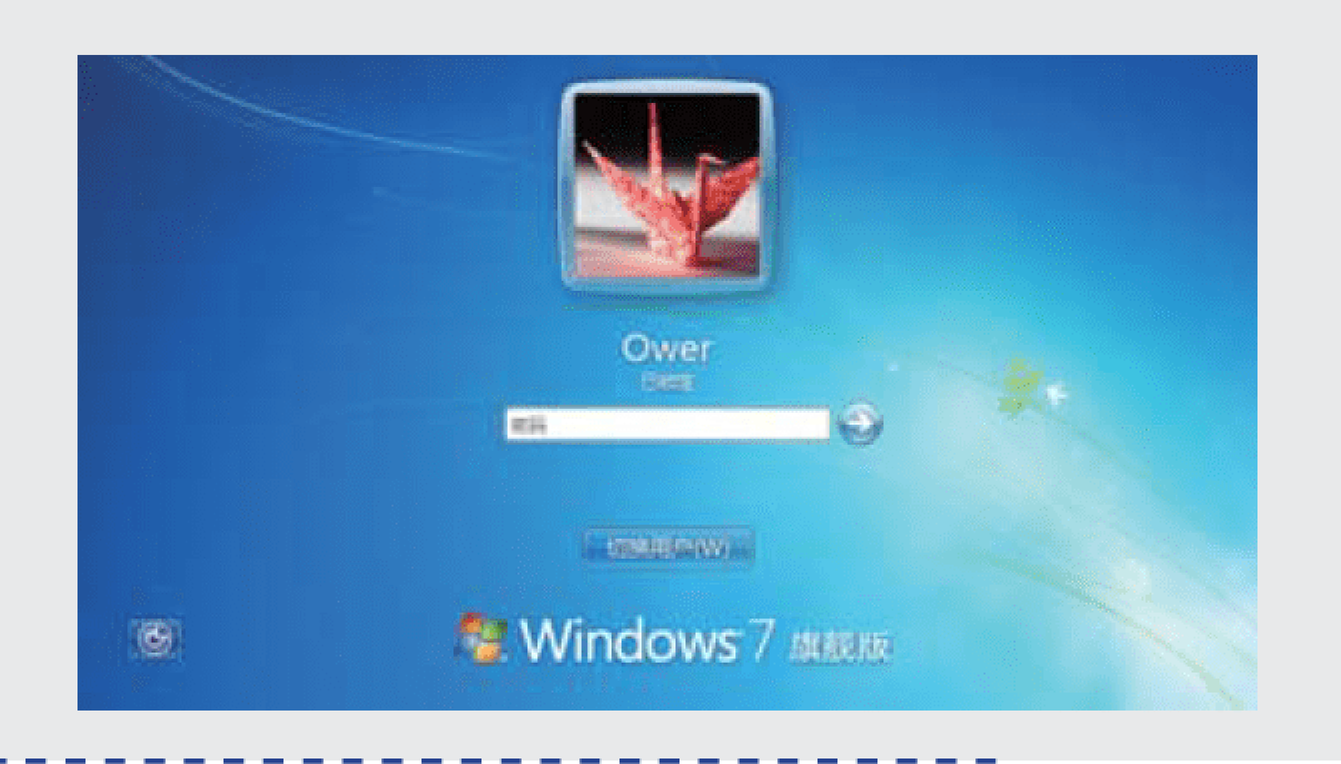
第2步：设置屏保及其启动密码

在打开对话框的“屏幕保护程序”下拉列表框中选择“彩带”选项，在“等待”数值框中输入“5”，然后选中“在恢复时显示登录屏幕”复选框，单击 确定 按钮保存设置。

教你一招

设置屏幕保护密码后，怎样重新登录系统？

在指定的时间内未对电脑进行操作时，系统将自动打开屏保，待重新进入系统时，将打开登录界面，输入正确的用户密码后即可进入系统。



8.2.3 设置电源管理密码

在操作系统中设置电源管理功能后，系统从节能状态返回时就会要求输入密码，从而在一定程度上实现保护系统的目的。



下面将在电源选项窗口中设置电源管理密码，其具体操作如下。



第1步：打开电源计划设置窗口

选择“开始”/“控制面板”命令，打开“控制面板”窗口，在其中单击“电源选项”超链接，在打开的窗口中选中“节能”单选按钮，然后单击右侧的“更改计划设置”超链接，打开设置窗口。



第2步：设置节能计划

在打开窗口的“关闭显示器”下拉列表框中选择“5分钟”选项，在“使计算机进入睡眠状态”下拉列表框中选择“15分钟”选项，然后单击 保存修改 按钮，返回上一界面。

第3步：设置密码保护

在其左侧窗格中单击“唤醒时需要密码”超链接，在打开的窗口中选中“需要密码”单选按钮，然后单击 保存修改 按钮保存设置。



提示：设置完成后，当电脑进入待机状态后重新唤醒时则打开登录界面，输入当前登录操作系统的用户账户密码后即可进入系统。



跟我练习

登录设置了密码的用户账户后设置其屏幕保护密码和电源密码

任务1：打开“屏幕保护程序设置”对话框，在其中将屏幕保护程序设置为“三维文字”，时间设置为“10分钟”，并设置恢复时显示登录屏幕。

任务2：将电源选项计划设置为“平衡”，关闭显示器时间设置为“10分钟”，使电脑进入睡眠状态时间设置为“10分钟”，并设置唤醒时需要密码。

屏幕保护程序(S)
三维文字 设置(T)... 预览(V)
等待(W): 10 分钟 在恢复时显示登录屏幕(R)

更改计划的设置：平衡
选择希望计算机使用的睡眠设置和显示设置。
关闭显示器: 10 分钟
使计算机进入睡眠状态: 10 分钟
更改高级电源设置(C)
还原此计划的默认设置(R)

8.3 常见办公文档的加密

今天娜娜收到公司总部传来的一份很重要的文件，她将其用Word文档保存下来，但是还是有些不放心，因为这份文件太重要了。她马上想到了阿伟，在娜娜的印象中阿伟对于电脑方面的知识很精通，于是就向阿伟请教怎样来处理这个文件让它更安全，阿伟了解了情况后告诉娜娜：“你要解决这个问题可通过对其设置密码来实现，下面我就来教你怎样为办公文档创建密码。”

8.3.1 设置Word文档的密码

Word是电脑使用中常用的应用软件之一，很多用户都用它来处理一些重要的文档，为了防止其他用户任意查看或篡改内容，可为Word文档设置保护密码。



下面将为Word 2010文档设置密码，其具体操作如下。

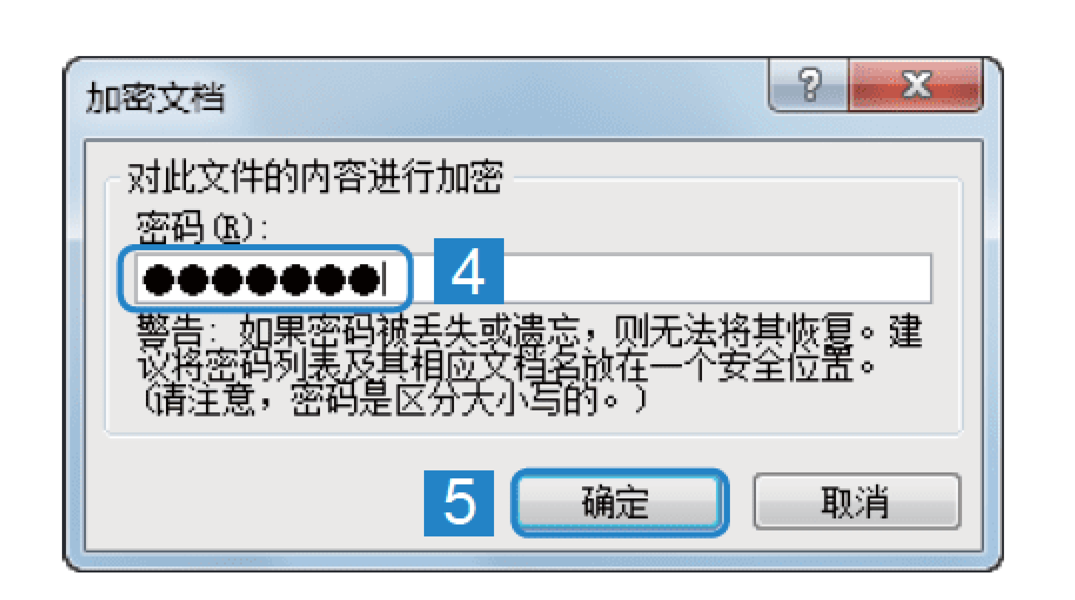


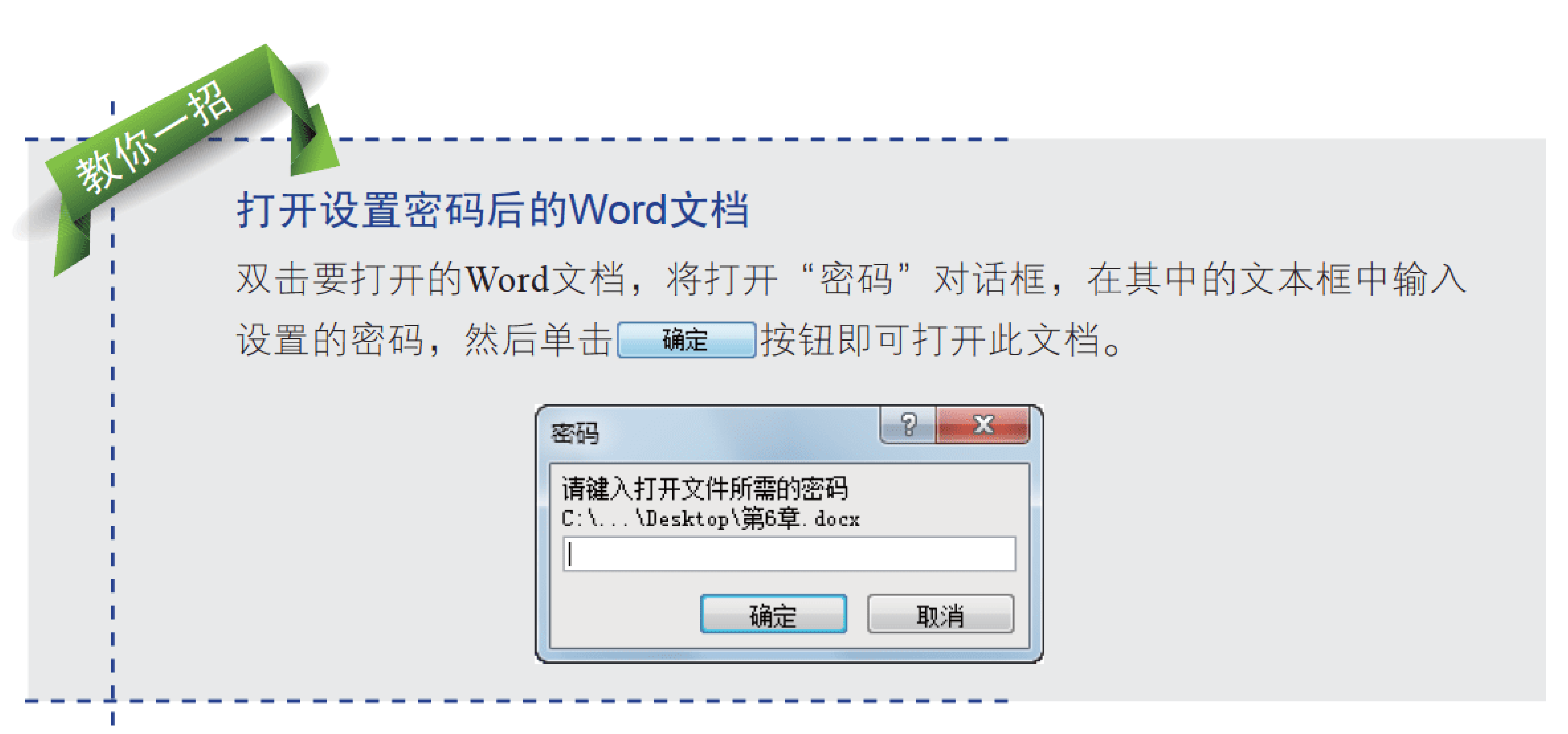
第1步：打开“加密文档”对话框

打开要进行加密的Word文档，然后选择“文件”选项卡，在其下方单击“保护文档”按钮，在打开的下拉列表框中选择“用密码进行加密”选项，打开“加密文档”对话框。

第2步：设置密码

在打开对话框的“密码”文本框中输入要设置的密码，然后单击 确定 按钮，系统提示再次输入密码，再次输入后单击 确定 按钮并保存设置即可。





打开设置密码后的Word文档

双击要打开的Word文档，将打开“密码”对话框，在其中的文本框中输入设置的密码，然后单击 确定 按钮即可打开此文档。

8.3.2 设置Excel文档的密码

Excel是Office办公软件的组件之一，使用它可进行强大的表格数据处理，在办公领域使用极为广泛。因此保障其数据安全就显得极其重要。用户可以通过为其设置打开权限密码来提高安全性。





下面将设置Excel 2010文档的密码，其具体操作如下。

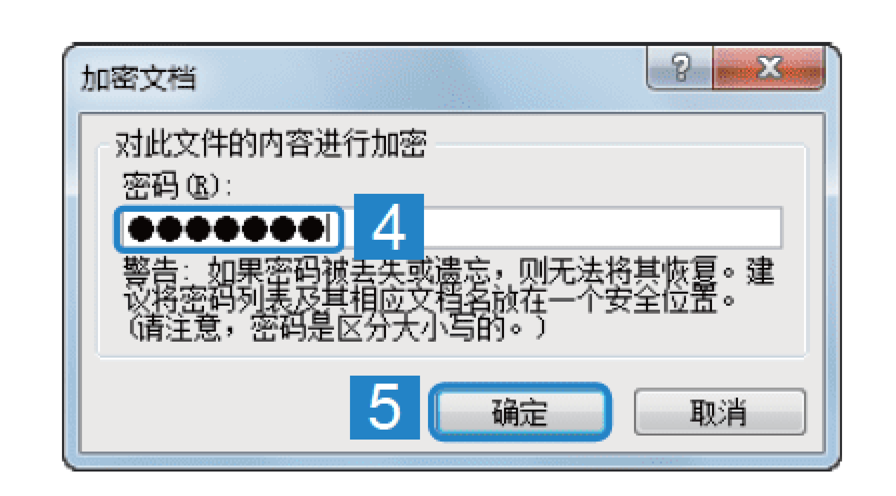


第1步：选择设置表格权限的类型

打开要设置权限的Excel表格，选择“文件”选项卡，在其下方单击“保护工作簿”按钮，在打开的下拉列表框中选择“用密码进行加密”选项，打开“加密文档”对话框。

第2步：设置密码

在打开对话框的文本框中输入要设置的密码，然后单击“确定”按钮，再次确认密码后对其设置进行保存即可。



教你一招

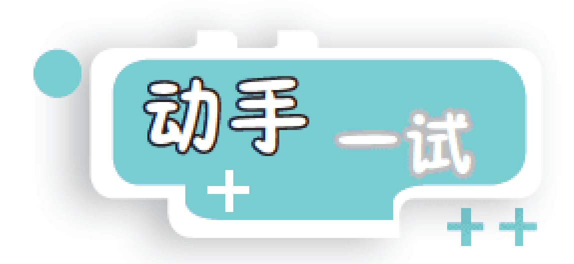
如何取消设置的Word和Excel密码？

要取消设置的Word和Excel文档密码非常简单，只需执行加密操作即可，其方法为：在打开的文件中选择“文件”选项卡，在其中选择“用密码进行加密”选项，在打开的“加密文档”对话框中将密码清空并确认设置即可。

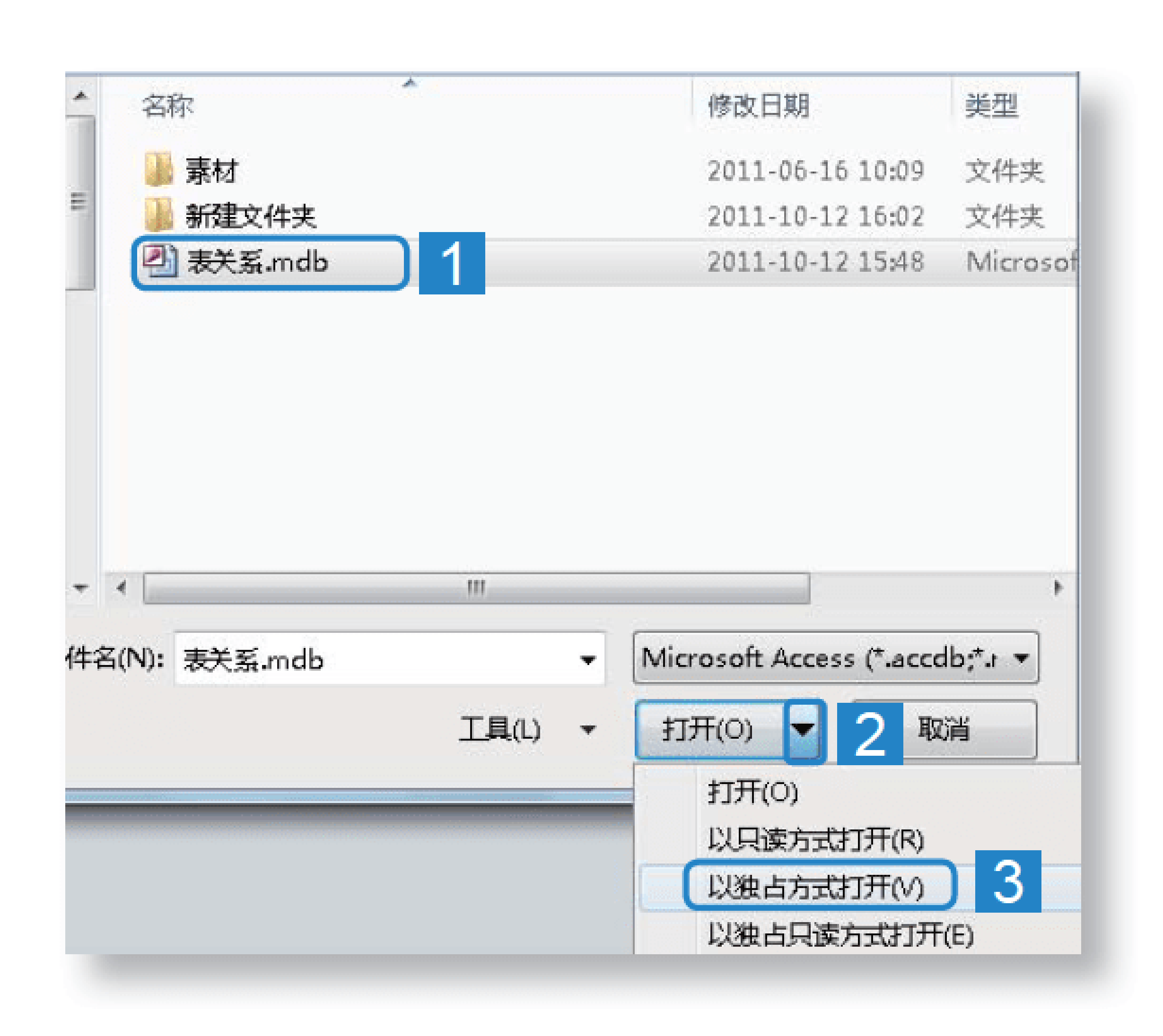


8.3.3 设置Access数据库密码

Access广泛应用于中小企业的数据库管理，其功能强大、灵活易用的特点深受用户好评。使用Access可以方便地管理和使用数据库，同时为了数据的安全，也可为其设置数据库密码。



要在Access 2010中设置其密码，必须“以独占方式打开”数据库才能进行设置，下面将对设置Access 2010密码的方法进行讲解，其具体操作如下。



第1步：打开要设置密码的数据库

选择“开始”/“所有程序”/Microsoft Office 2010/Microsoft Access 2010命令，启动Access程序，在“文件”选项卡中单击“打开”按钮，在打开的对话框中选择要打开的文件，然后单击打开(O)按钮右側的按钮，在打开的下拉菜单中选择“以独占方式打开”命令。

第2步：打开密码设置对话框

在打开的数据库中选择“文件”选项卡，在其下方单击“设置数据库密码”按钮，打开“设置数据库密码”对话框。



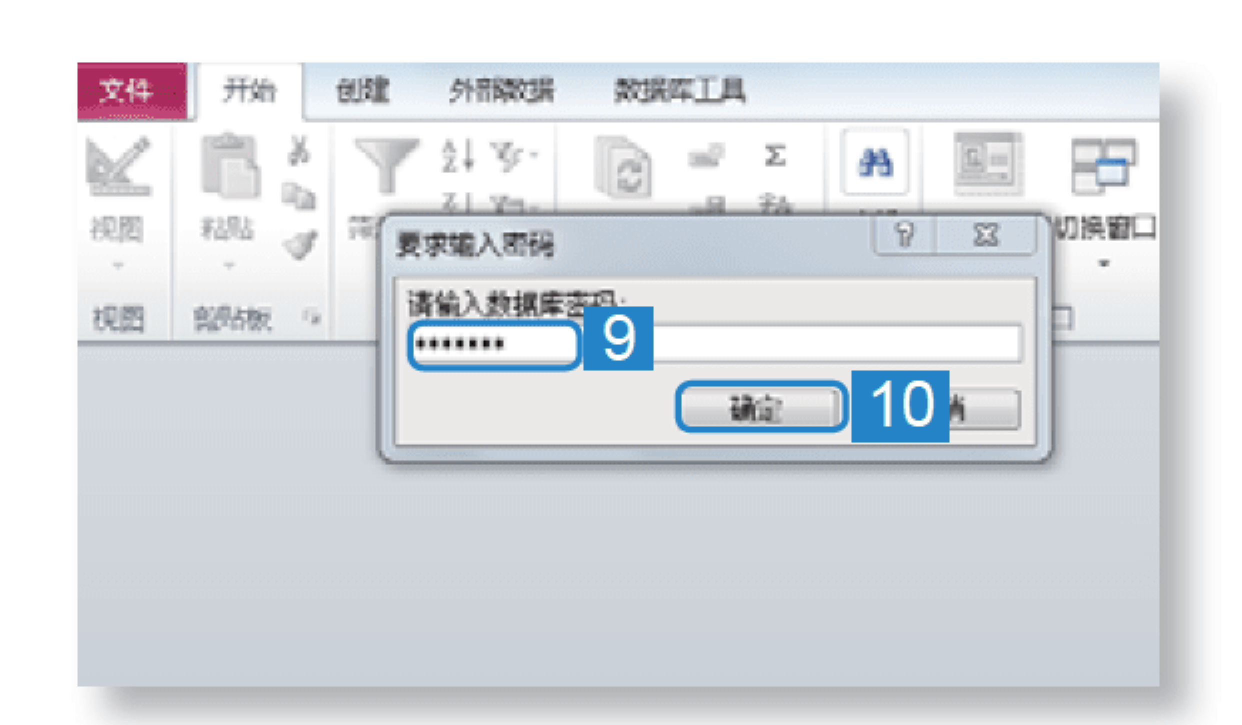
提示：在该选项卡中单击“用户和权限”按钮，在打开的下拉菜单中选择相应选项也可对数据库进行加密。



第3步：设置密码

在打开对话框的“密码”文本框中输入要设置的密码，在“验证”文本框中再次输入密码，然后单击 确定 按钮即可。





第4步：打开设置密码后的数据库文件

双击数据库文件图标，即可打开密码提示框，在其中输入设置的密码，然后单击 确定 按钮即可打开数据库。

教你一招

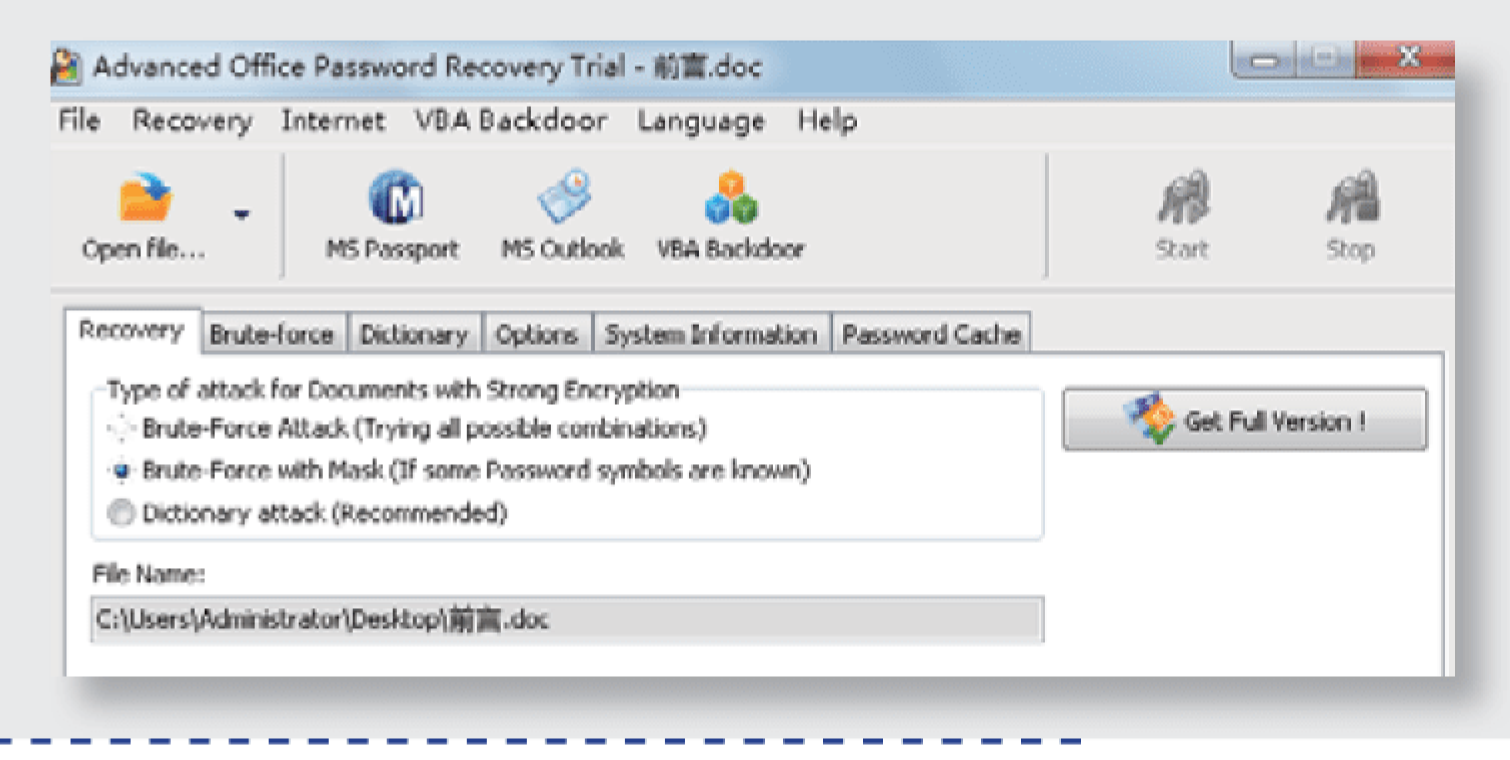
如何清除数据库的密码

要清除设置的数据库密码，可重新打开“设置数据库密码”对话框，在其中将密码清空，然后确定设置即可。

教你一招

使用Advanced Office Password Recovery Trial软件破解文档密码

上网下载Advanced Office Password Recovery Trial软件，然后启动该软件，在其中单击按钮添加要破解密码的Office文档，根据提示进行操作即可查看到文档的破解信息。





8.4　文件及文件夹加密

娜娜听了阿伟前面的讲解，她想：“阿伟所教她设置文档密码的方法并不是对所有的文件都有用，如果要对其他类型的文件进行加密，那该怎么办呢？”于是她又找到阿伟告诉他自己的疑问，阿伟听了以后笑着说：“我正要给你补充这些知识呢，别着急，下面就给你讲解！”

8.4.1　文件及文件夹加密的方法

在日常的电脑使用中，为文件和文件夹加密是非常常见的操作之一，通过加密能很好地保证文件的安全性，加密的方法有很多，这些加密的方法有各自的优点，但也有无法避免的缺点，有的加密速度快，有的加密速度相对比较慢，但加密速度快的通常没有加密速度慢的加密强度高。



下面将介绍对文件和文件夹最常见的几种加密方法及其特点。



- **系统自带的加密功能：** 在操作系统中可通过文件或文件夹属性窗口对其进行加密，也可通过改变文件的扩展名或隐藏文件及文件夹实现与加密相同的效果，这种加密方式具有操作简单、实用性强且安全性高的特点。
- **通过压缩软件进行加密：** 在操作系统中可将要加密的文件和文件夹添加为压缩文件，利用压缩软件的加密功能对其进行加密。这样既方便用户操作，又能保证文件数据的安全性。
- **通过专业的加密软件进行加密：** 使用专业的加密软件进行加密是一种对文件夹快速加密的方法，它对文件夹的大小没有限制，并且加密和解密的速度快。其加密安全度是几种方法中最高的。

8.4.2 使用系统自带的加密功能进行加密

资料文件存储在电脑中，很多情况下电脑都是多人共用的，那么，如何给文件夹加密，让其他人无法浏览这些资料内容呢？这里将介绍几种常用的无须安装软件，操作系统自带的加密方法。

1. 修改文件的扩展名

将文件的扩展名（也就是文件名最后的几个字母，如文件名“第3章.doc”的“.doc”）改为其他任意名称，文件夹需压缩后再更改，更改后用户将无法打开文件进行查看。



下面将以更改“资料.doc”文件扩展名为“资料.abc”为例进行讲解，其具体操作如下。

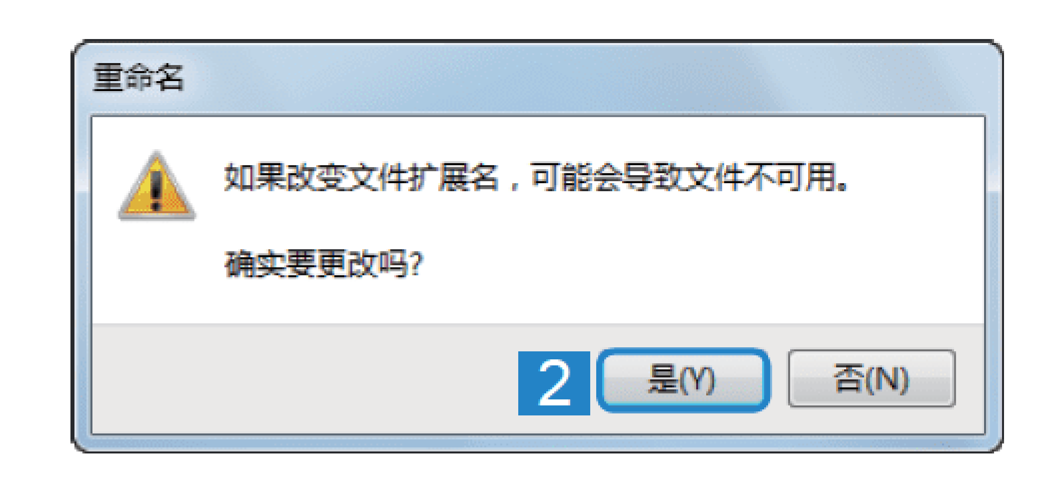


第1步：选择“重命名”命令

在要进行修改的文件“资料.doc”图标上单击鼠标右键，在弹出的快捷菜单中选择“重命名”命令，使文件名呈可编辑状态。

第2步：修改文件扩展名

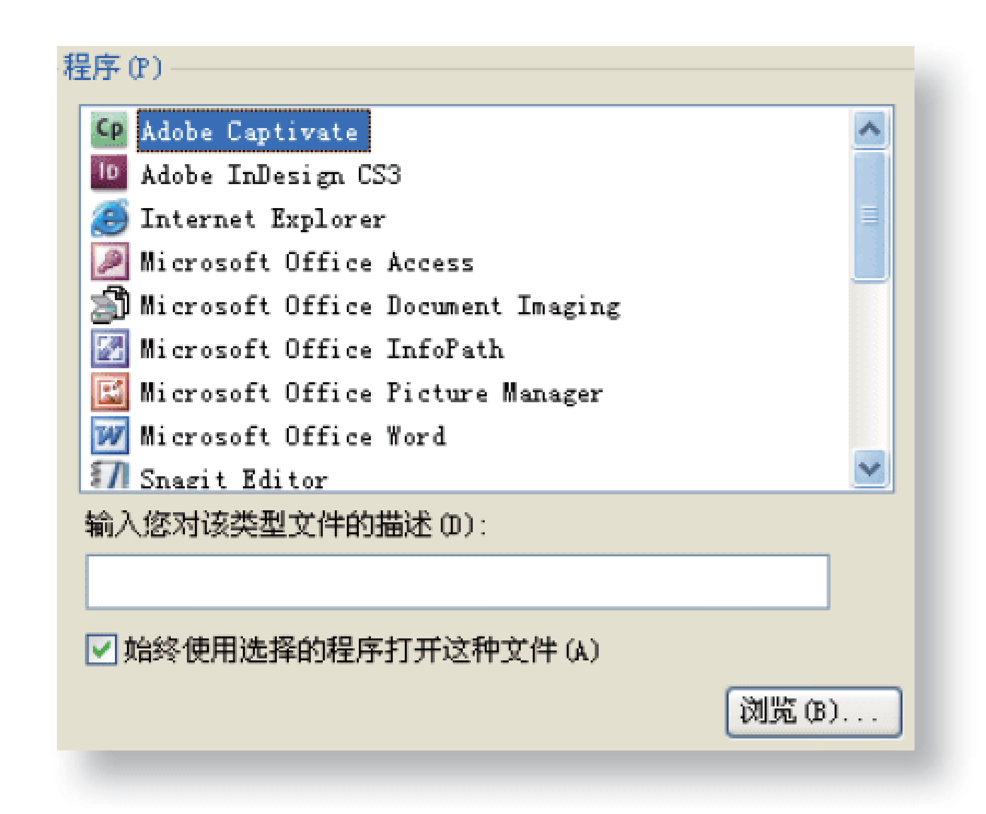
选中其中的“.doc”文本，将其修改为“.abc”，然后在打开的“重命名”对话框中单击 是(Y) 按钮确认修改。



提示：在修改文件的扩展名之前，一定要将其记住后再更改，如果需要查看文件，则恢复原来的扩展名即可。

第3步：打开文件后的效果

修改文件扩展名后，双击该文件，将打开提示对话框提示无法打开该文件，可选择浏览电脑中的程序进行打开，即不能使用其他任何程序打开。

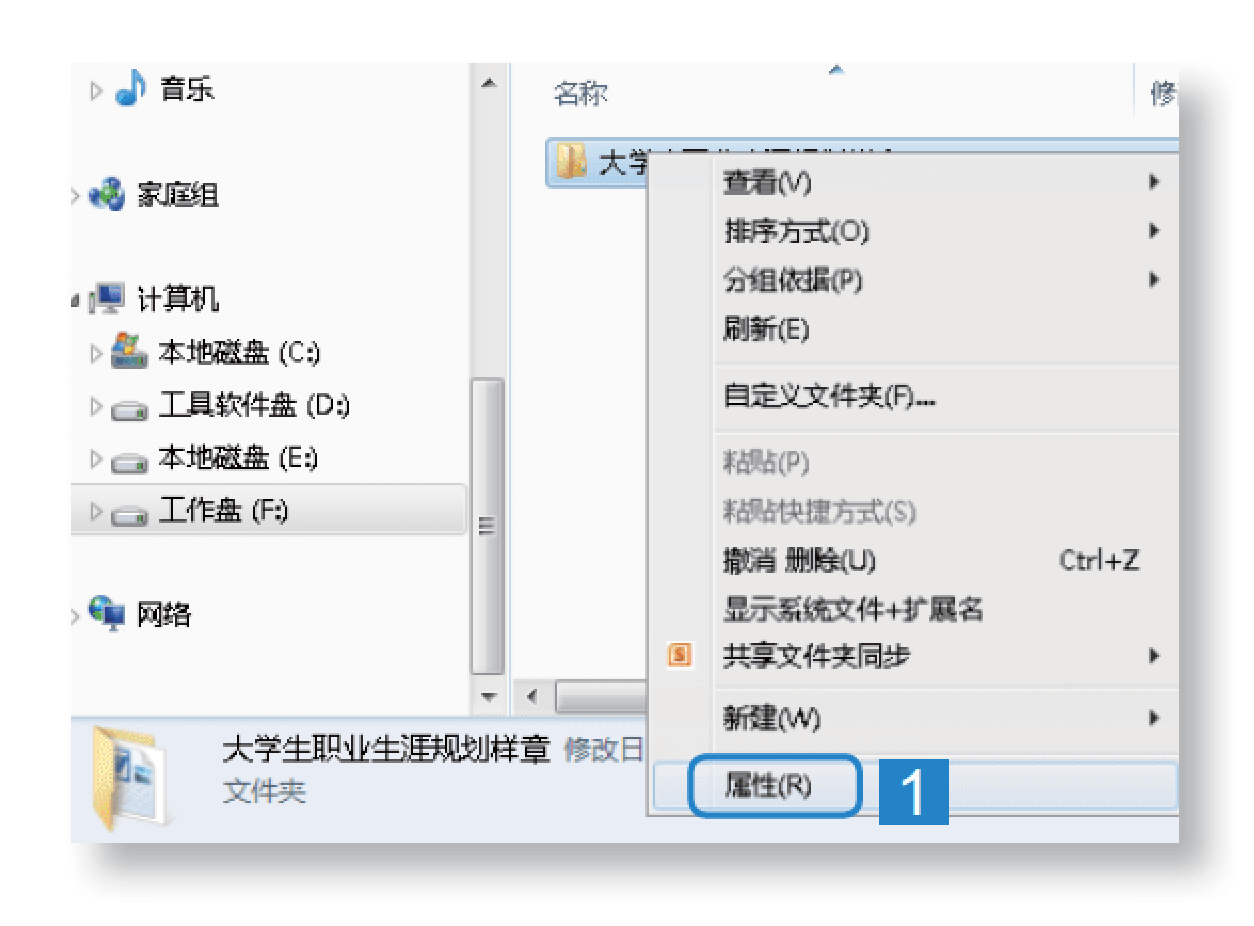


2. 使用文件属性对话框加密文件

在操作系统中可利用文件属性对话框对文件进行加密保护，这种加密方式不仅简单易于操作，而且是操作系统最直接的加密方法。



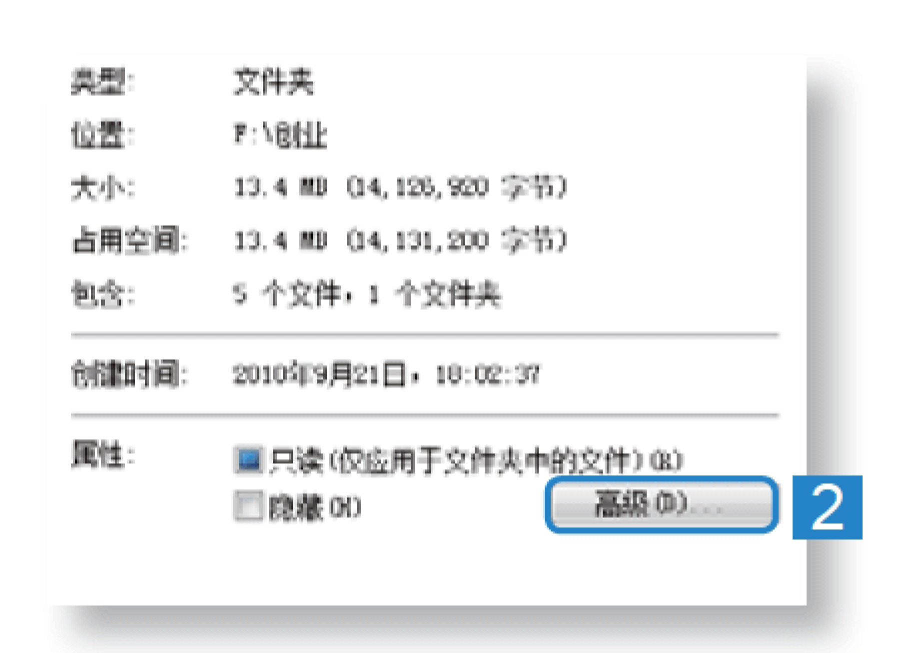
下面将在“Windows资源管理器”窗口中加密文件，其具体操作如下。



第1步：打开文件属性对话框

打开“Windows 资源管理器”窗口，在其中要进行加密的文件夹上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令。



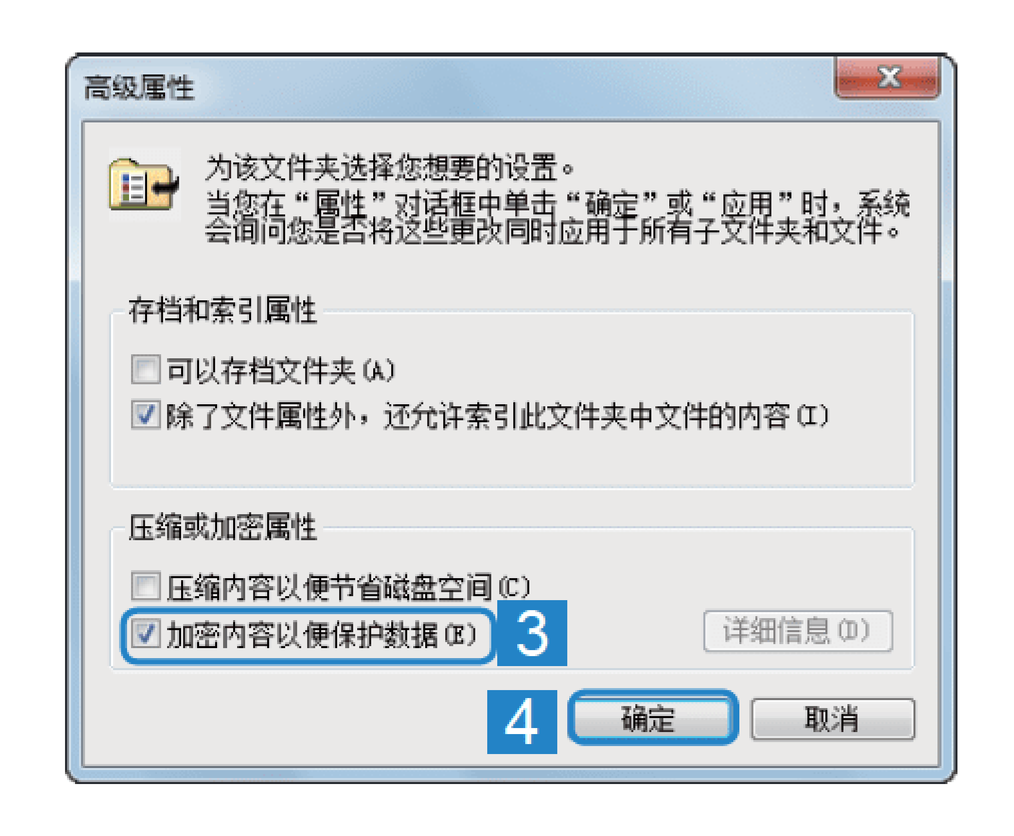


第2步：打开“高级属性”对话框

在打开的对话框中显示了该文件的基本信息，单击 高级(D)... 按钮，打开“高级属性”对话框。

第3步：加密设置

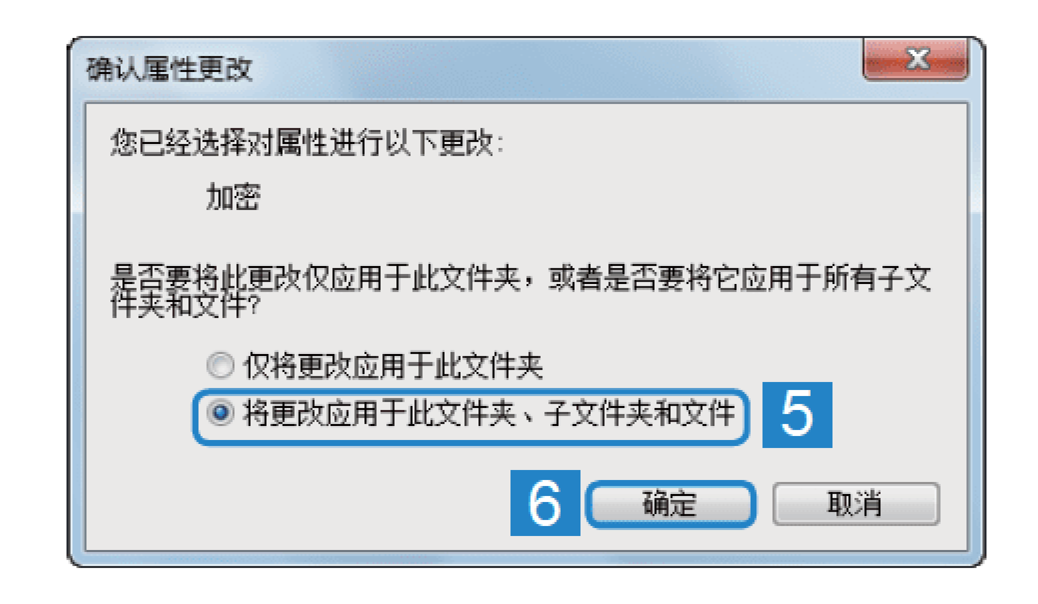
在打开的对话框中选中“加密内容以便保护数据”复选框，然后单击 确定 按钮确认设置。



提示：加密后，用户使用其他账户登录电脑或重装系统后将无法查看文件内容。

第4步：应用设置

返回文件属性对话框，单击 确定 按钮，系统将打开“确认属性更改”对话框，保持默认设置，单击 确定 按钮完成加密。



新手解惑

Q：使用这种方式在加密过程中应注意哪些问题？

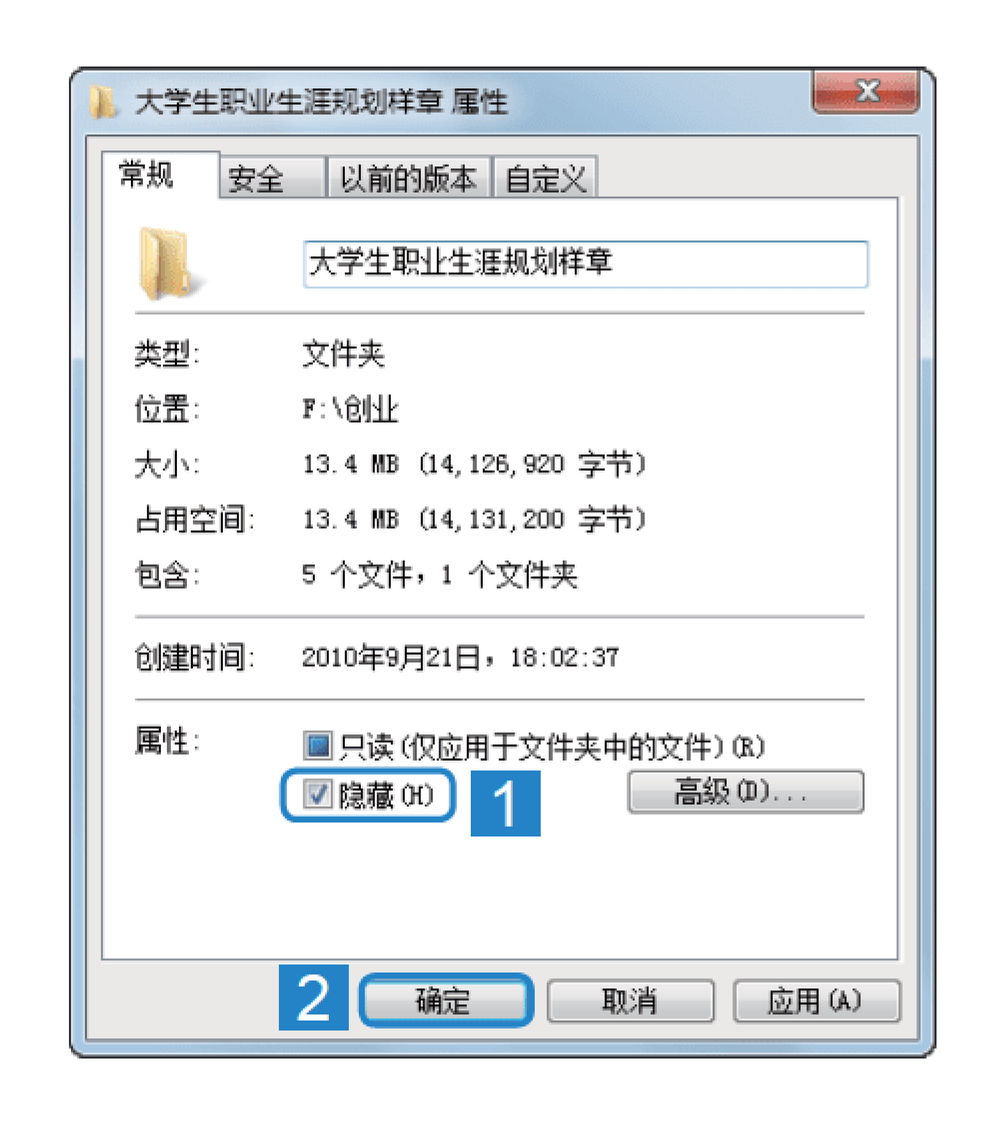
A：只可以加密NTFS格式分区的文件和文件夹，FAT分区卷上的文件和文件夹无效。被压缩的文件或文件夹也可以加密，如要加密一个压缩文件或文件夹，则该文件或文件夹将会被解压。无法加密标记为“系统”属性的文件，并且位于systemroot目录结构中的文件也无法加密。

3. 隐藏文件和文件夹

将文件或文件夹属性设置为隐藏文件，再将文件和文件夹的查看方式设置为“不显示隐藏的文件或文件夹”，即可实现文件与文件夹的保护，该操作可结合修改文件扩展名和使用文件属性对话框加密文件进行使用。



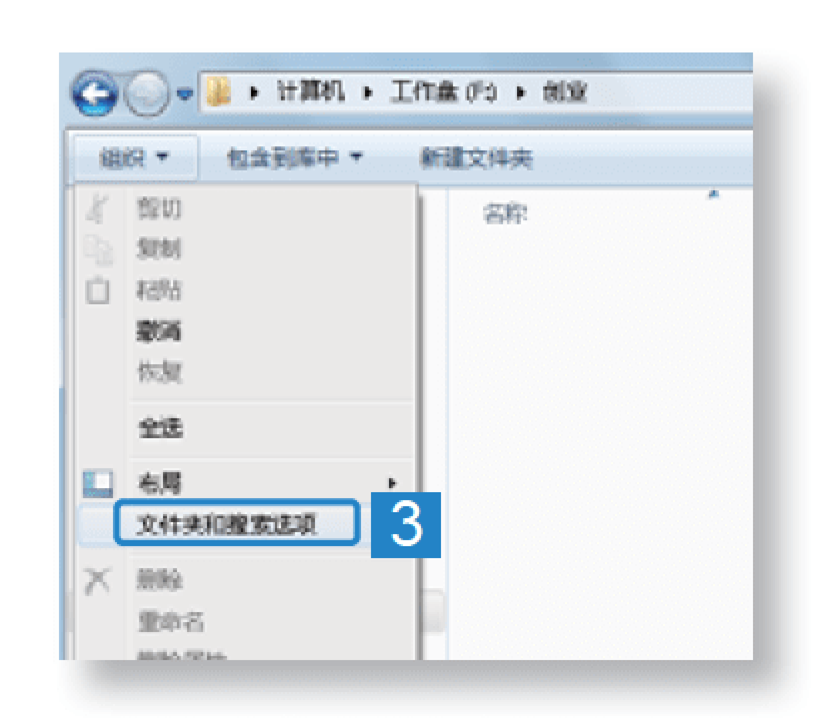
下面将文件夹进行隐藏并设置不显示隐藏文件。



第1步：隐藏文件夹

在加密后的文件上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，打开属性对话框，在其“属性”栏中选中“隐藏”复选框，然后单击确定按钮隐藏该文件夹。

提示：隐藏文件夹后，如系统默认的是显示隐藏文件夹，则该文件夹仍然显示在其中并呈浅色显示。

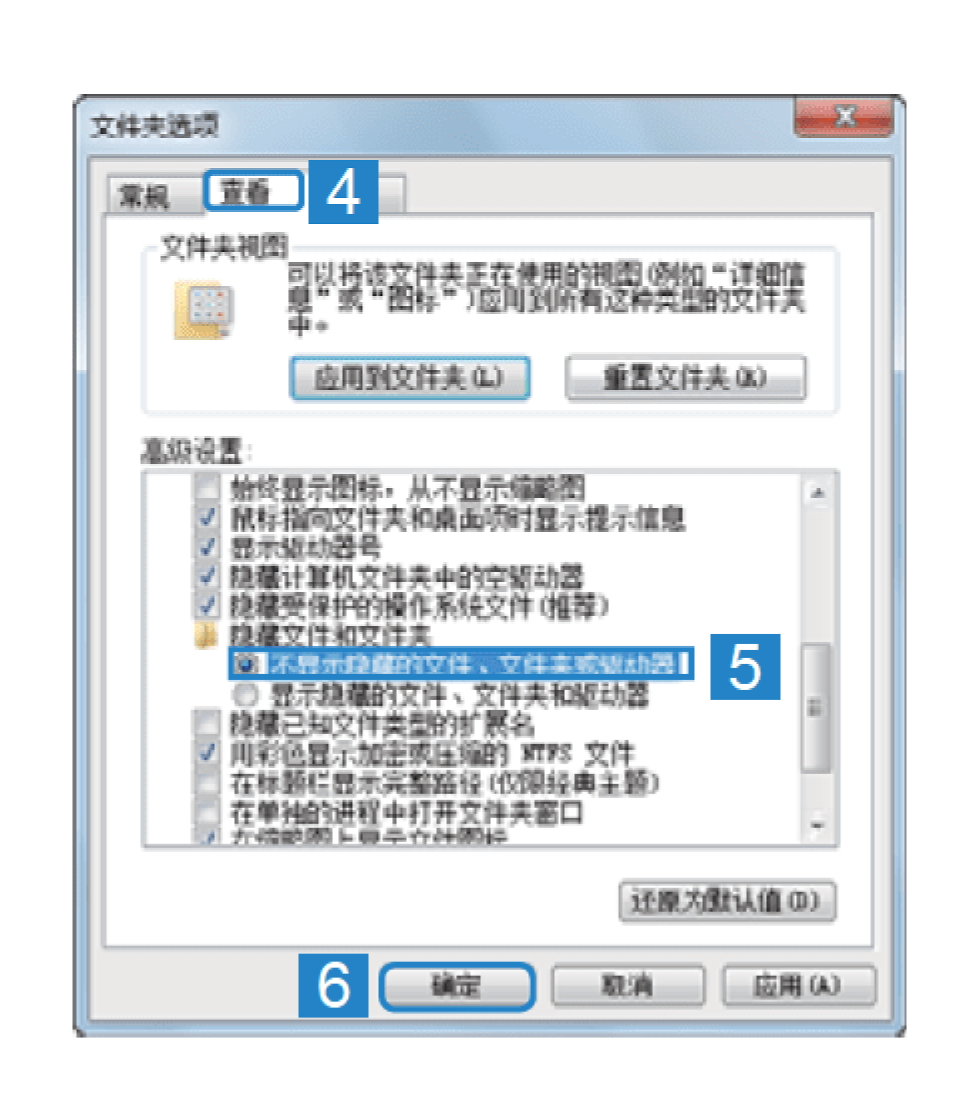


第2步：打开“文件夹选项”对话框

打开资源管理器，在其中选择“组织”/“文件夹和搜索选项”命令，打开“文件夹选项”对话框。

第3步：设置不显示隐藏的文件夹

在打开的对话框中选择“查看”选项卡，然后在“高级设置”下拉列表框中选中“不显示隐藏的文件、文件夹或驱动器”单选按钮，最后单击确定按钮即可应用设置。





8.4.3 使用压缩软件加密文件和文件夹

将文件或文件夹压缩成加密压缩文件可保护文件和文件夹不被他人访问，用户在压缩文件时对其进行设置密码后再开始压缩，则所得到的压缩文件将带有密码保护。



下面将在安装有压缩软件的操作系统中将目标文件压缩为带密码的压缩文件，其具体操作如下。

第1步：添加压缩文件

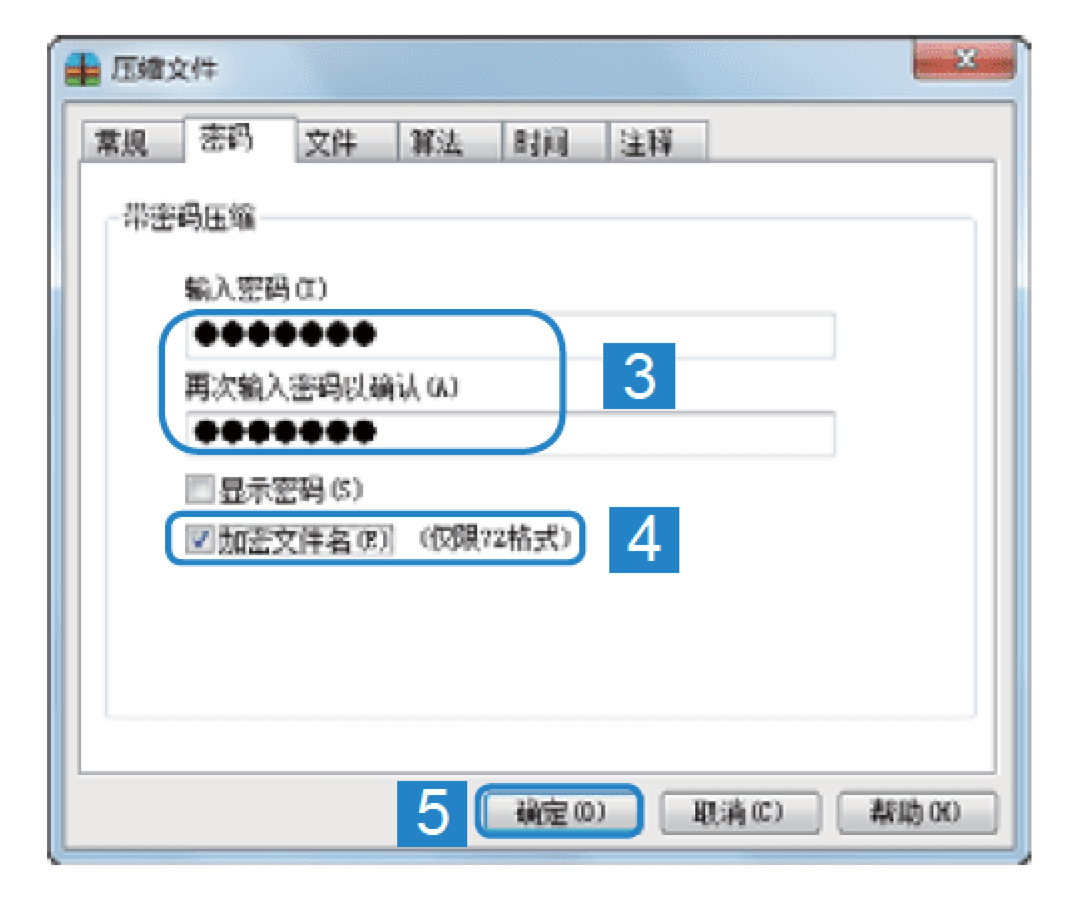
在要添加为压缩文件的文件夹图标上单击鼠标右键，在弹出的快捷菜单中选择“添加到压缩文件”命令，打开“压缩文件”窗口。



第2步：设置要压缩文件的密码

在打开窗口的“常规”选项卡的“压缩文件格式”栏中选中7Z单选按钮。





第3步：设置压缩文件的密码

选择“密码”选项卡，在“带密码压缩”栏的文本框中分别输入相同的密码，选中“加密文件名”复选框，然后单击 确定 按钮，系统将自动进行文件的压缩。

第4步：打开压缩文件

创建压缩文件后，双击其图标，将打开提示对话框提示输入密码，输入密码后单击 确定 按钮即可将其打开。



新手解惑

Q：使用压缩软件加密为什么要将其格式设置为7Z?

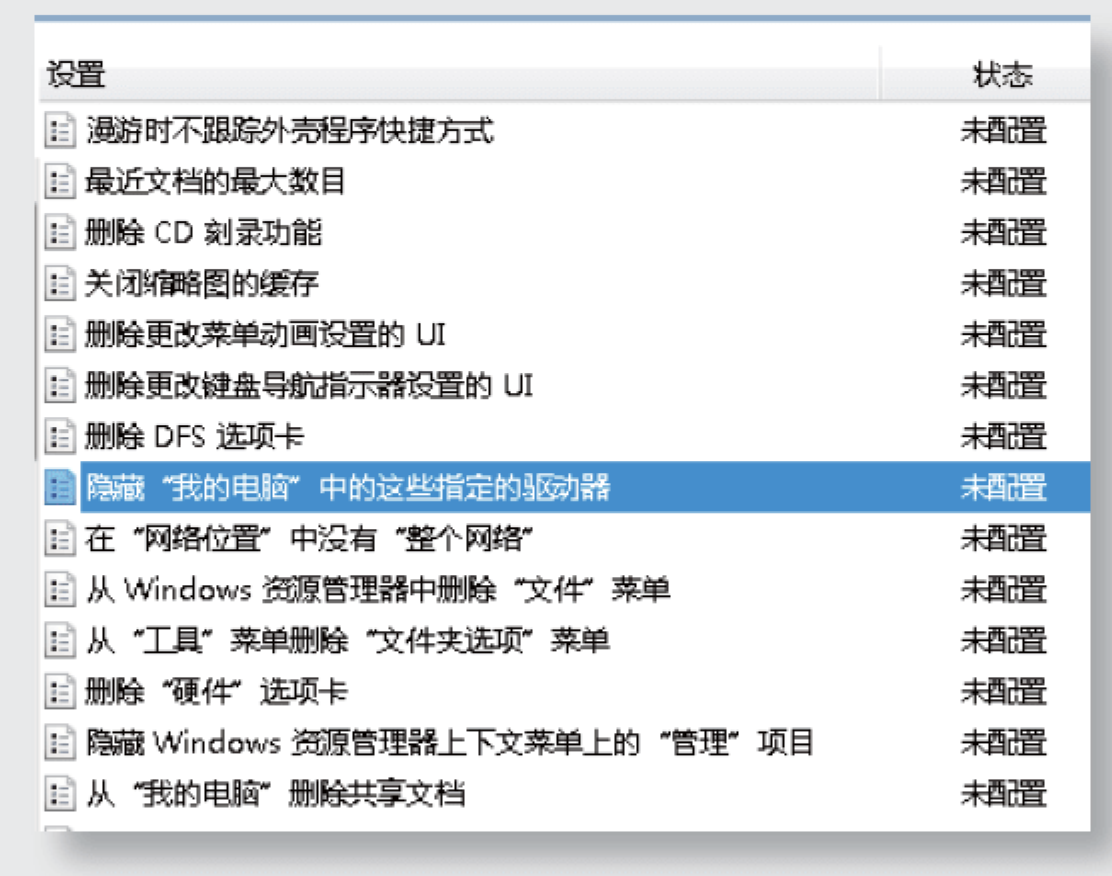
A：在打开的压缩软件界面中，只有将其压缩的格式设置为7Z，在“密码”选项卡的“输入密码”文本框才成可编辑状态。

教你一招

将重要文件“藏”起来

一般来说普通用户打开电脑，总是很自然地去硬盘分区中翻来翻去，因此将重要文件隐藏起来，是一项数据保密的好办法。除隐藏文件外，还可以直接隐藏硬盘分区。

隐藏分区的方法为：打开本地组策略编辑器，依次展开“用户配置/管理模板/Windows组件/Windows资源管理器”选项，双击“隐藏‘我的电脑’中的这些指定的驱动器”选项，在打开的对话框中选中“已启用”单选按钮，在其选项的下拉列表框中选中要隐藏的驱动器选项即可。

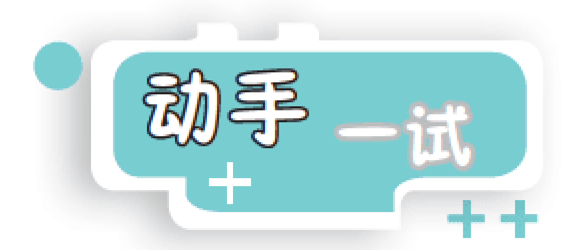






8.4.4 使用文件夹加密超级大师加密文件

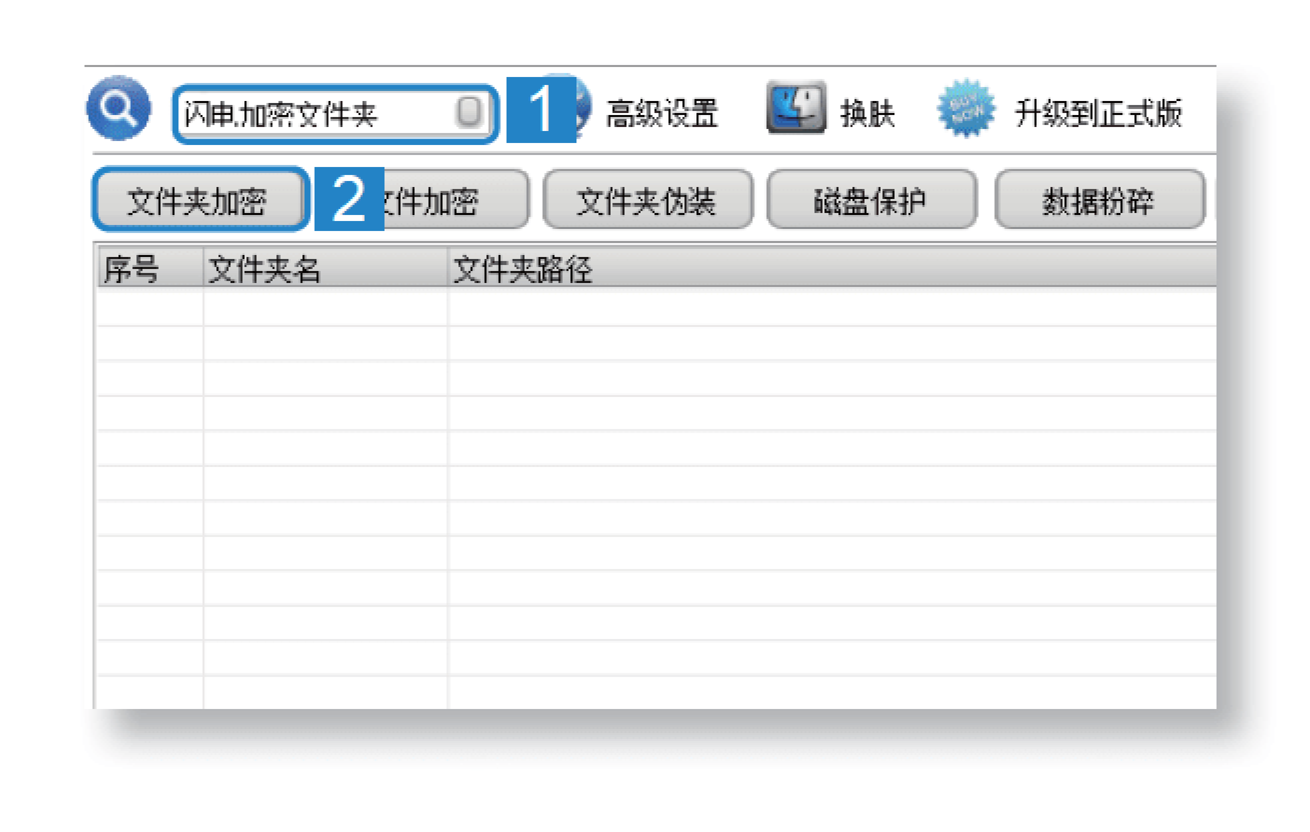
使用文件夹加密超级大师能加密电脑里或移动硬盘上的文件和文件夹，无大小限制，加密后可防止复制和删除，并且不受系统影响，即使重装、Ghost还原、DOS和安全模式下，加密的文件夹依然保持加密状态，在何种环境下通过其他软件都无法解密。



下面将使用安装的文件夹加密超级大师软件（下载地址为http://www.cksis.com/down_New_Soft/FSESetup.zip）加密电脑中的“素材”文件夹，其具体操作如下。

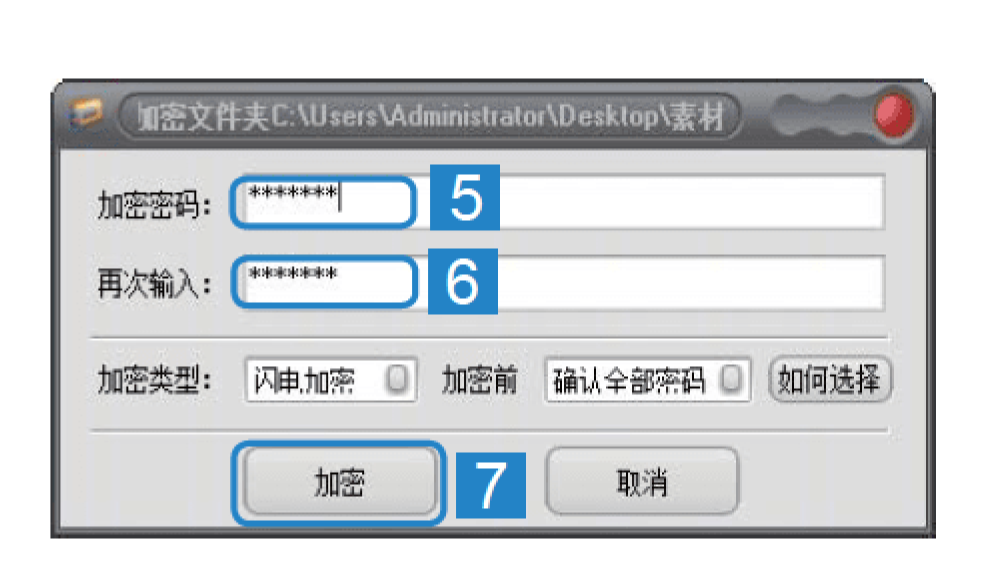
第1步：设置加密方式

启动文件夹加密超级大师软件，在其主界面的下拉列表框中选择文件夹的加密方式，这里选择“闪电加密文件夹”选项，然后单击[文件夹加密]按钮，打开“浏览文件夹”对话框。



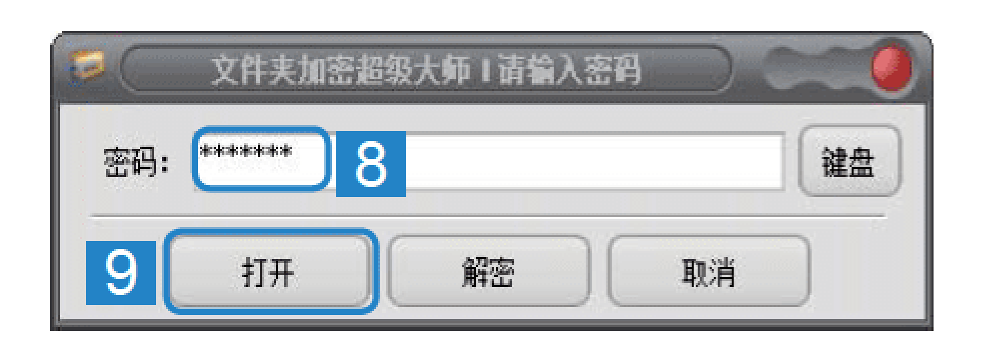
第2步：选择要进行加密的文件夹

在打开对话框的列表框中选择“素材”文件夹，然后单击[确定]按钮，打开密码设置对话框。



第3步：设置密码

在打开对话框的“加密密码”和“再次输入”文本框中输入要设置的密码，然后单击[加密]按钮即可为文件夹加密。



第4步：打开已加密文件夹

双击已加密的文件夹图标，在打开的对话框中输入设置的密码，单击 打开 按钮即可打开该文件夹。

教你一招

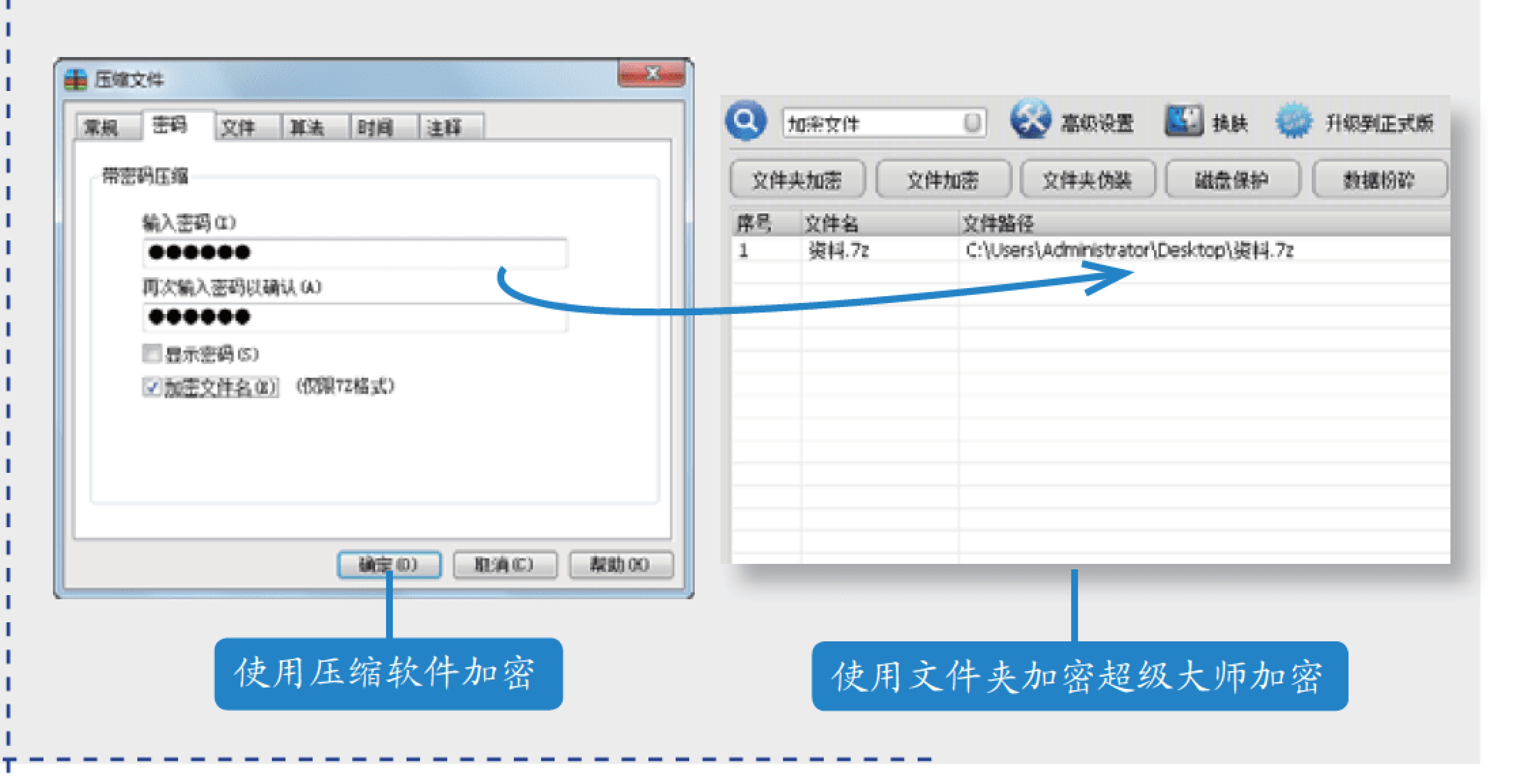
文件夹加密超级大师的其他作用

使用文件夹加密超级大师除可对文件和文件夹进行加密外，还可以使用其对磁盘进行保护，其方法为：在打开的软件主界面中选择加密的磁盘，然后单击 磁盘保护 按钮，根据向导即可完成其操作 。

跟我练习

将电脑中的重要文件进行加密

娜娜通过前面的学习，决定将自己电脑中重要的软件进行加密处理，首先将所有重要资料放入一个文件夹中，然后使用添加压缩软件的方法为该文件进行加密处理，再使用文件夹加密超级大师再次对文件进行加密，使文件具有双重加密。



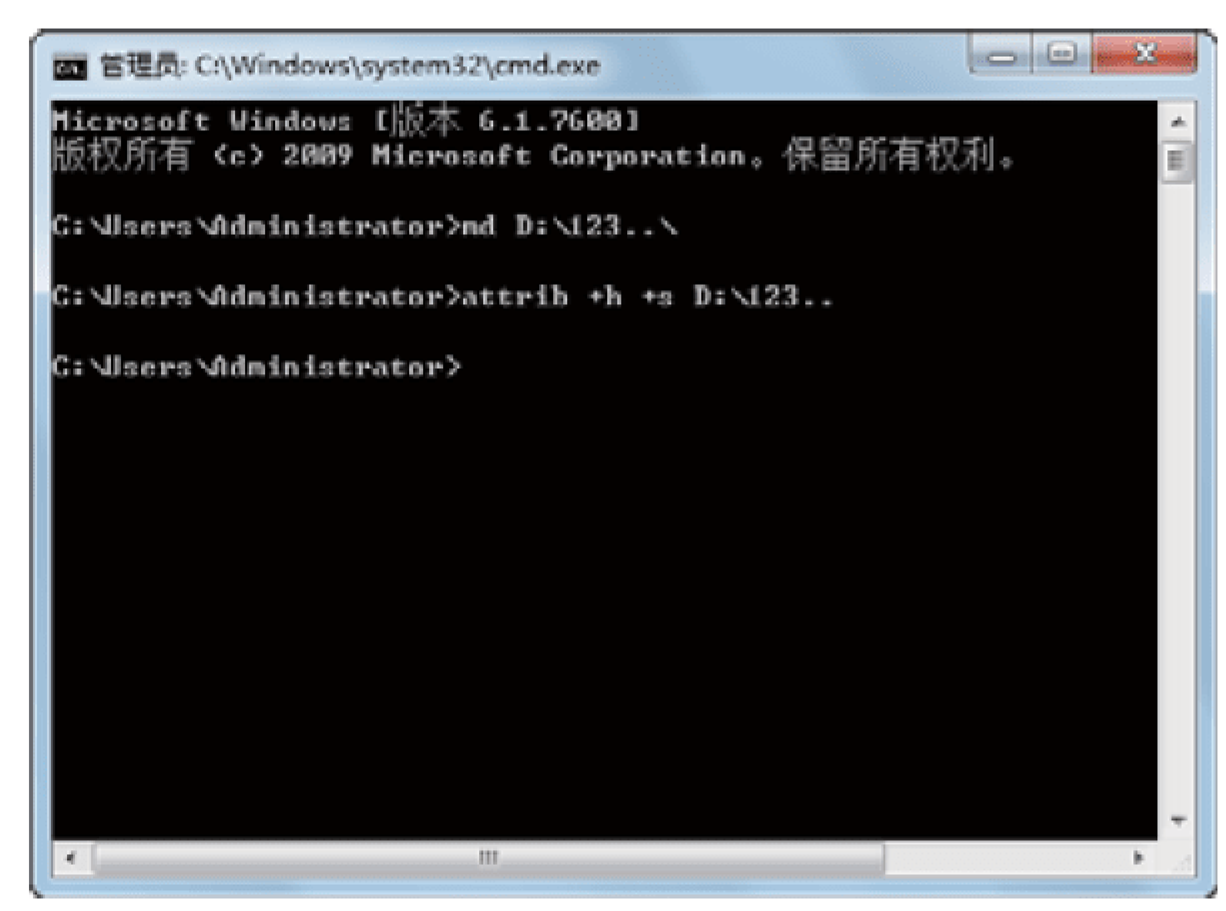


8.5 使用命令提示符创建安全文件夹

阿伟告诉娜娜：“在命令提示符窗口中使用命令可创建一个正常情况下不能删除的文件夹，这样能防止他人破坏文件，为了保证其安全性，还可将其进行深度隐藏。”娜娜听了阿伟所说的以后似乎对这很感兴趣，立即要求阿伟为她讲解。



下面将在命令提示符窗口下使用命令在D盘中建立一个名为“123”的文件夹并将其隐藏，其具体操作如下。



第1步：创建文件夹

选择“开始”/“运行”命令，在打开的对话框中执行cmd命令，打开命令提示符，在其中执行“md D:\123..\”命令创建文件夹。

提示：要打开该文件夹，可在“运行”对话框中执行“D:\123..\”命令。

第2步：隐藏创建的文件夹

在命令提示符窗口中输入“attrib +h +s D:\123..”命令，即可隐藏该文件夹。

提示：要重新显示隐藏的文件夹，可在命令提示符中执行“attrib -h -s D:\123..”命令。

教你一招

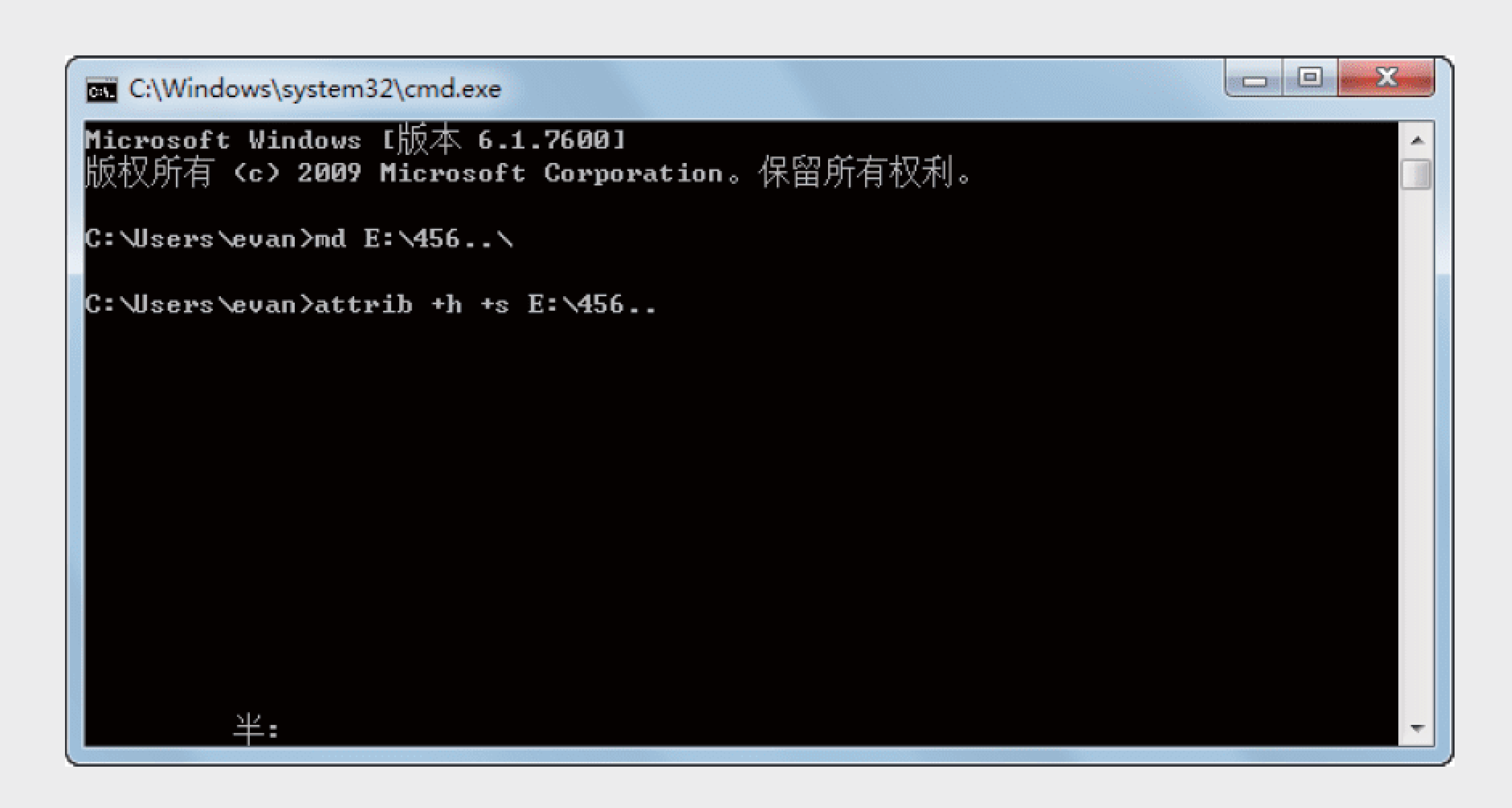
删除使用命令创建的文件夹

要删除创建的文件，其方法为：打开命令提示符，在其中执行“rd D:\123..\”命令即可。

跟我练习

在E盘中使用命令创建文件夹并进行深度隐藏

选择“开始”/“运行”命令，在打开的对话框中执行cmd命令，打开命令提示符。在其中首先执行“md E:\456..\”命令创建文件夹，将要保存的文件放入该文件夹中，然后执行“attrib +h +s E:\456..”命令隐藏该文件夹。



8.6 更进一步——轻松保护电脑安全

阿伟感觉娜娜对电脑密码的设置很感兴趣，他想这可能是娜娜已经对自己电脑的安全失去信心了吧，她这样热衷于学习密码的相关知识也许是为了防止电脑不再出现安全问题，想到这里，他决定再给娜娜总结一些简单有效保护电脑安全的设置。

第1招 为电脑设置两个密码



用户可在电脑中为操作系统设置两个密码，一个为管理员密码，一个为普通用户密码，这样可保证其他人登录电脑的权限得以控制。其设置方法如下：

①进入管理员账户，为其添加一个标准用户。

②分别为管理员账户和新建账户设置密码，并设置新建用户的使用权限。

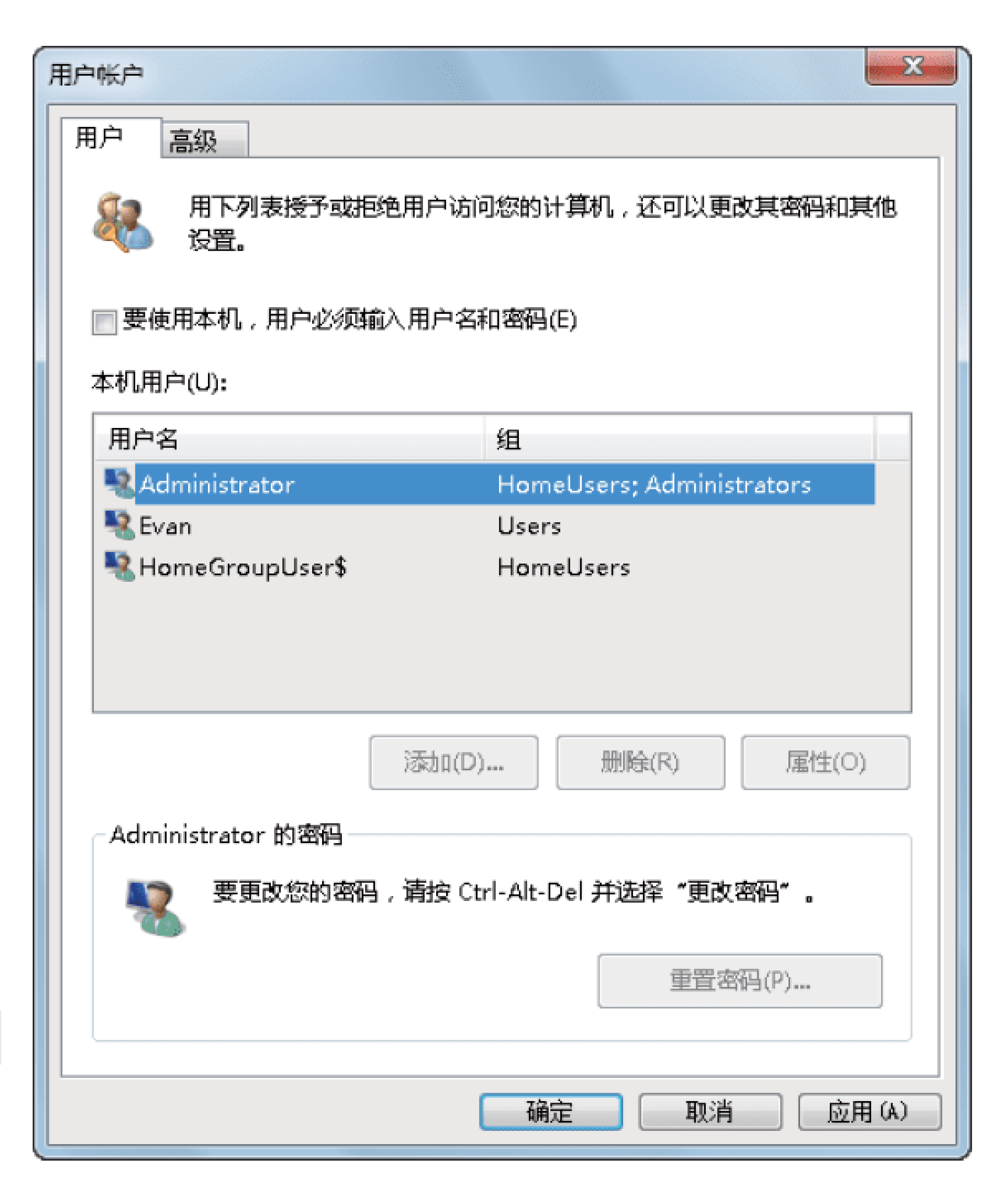


第2招 设置密码后Windows 7也可以自动登录

用户在电脑中设置系统账户密码后，为了不在启动系统时显示账户列表，可设置直接自动登录用户账户，以防止他人使用管理员账户进入系统更改相关设置，其方法如下：

①按Win+R键，打开“运行”窗口，执行“control userpasswords2”命令，打开“用户帐户”窗口，选择指定用户，取消选中“要使用本机，用户必须输入用户名和密码”复选框，然后单击确定按钮。

②在打开的“自动登录”对话框中输入该账户对应的密码，然后单击确定按钮即可完成设置。

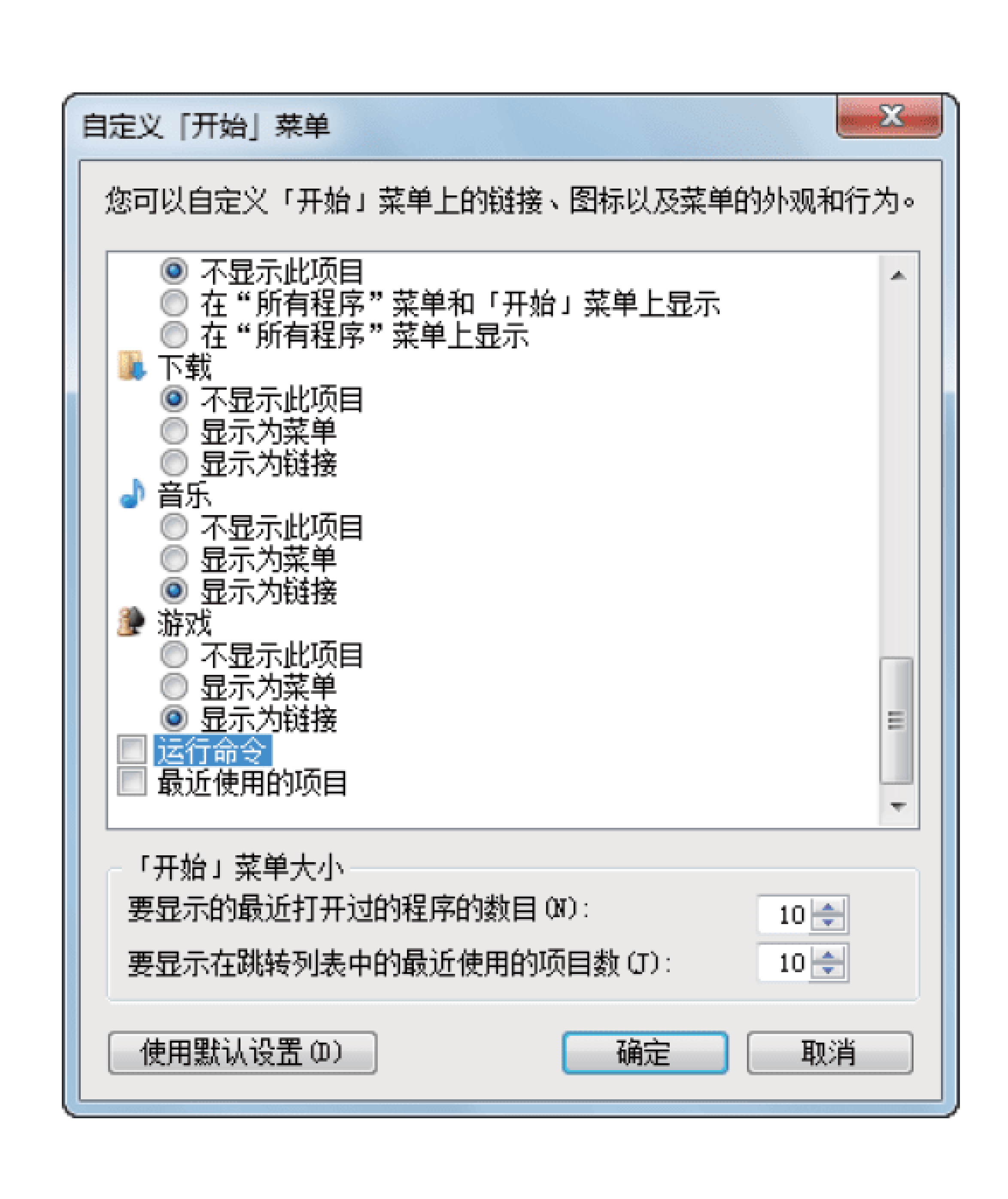


第3招 隐藏Windows 7的“运行”命令

在Windows 7操作系统中，如果“运行”命令存在于“开始”菜单中，这样将使电脑处于危险的状态。由于系统的很多操作都可通过它来进行，因此，可将其隐藏，其方法如下：

①单击“开始”按钮，打开其菜单，在其空白处单击鼠标右键，然后在弹出的快捷菜单中选择“属性”命令。

②在打开的对话框中单击自定义(C)...按钮，在打开的“自定义「开始」菜单”对话框的下拉列表框中取消选中“运行命令”复选框，然后单击确定按钮即可隐藏“运行”命令。



8.7 活 学 活 用

（1）简述在电脑中设置相关密码时，应设置怎样的密码才能使其更具安全性，使用密码时应注意哪些方面的问题。

（2）分别通过组策略和注册表加强密码的安全性，并限制密码格式。

（3）上网搜索并下载文件夹加密软件，然后学习使用加密软件对电脑中的文件夹进行加密。

（4）在系统中通过使用文件夹属性和添加压缩文件的方法将保存的图片文件进行加密。

（5）使用学过的方法将电脑中重要的Word文档、Excel表格以及数据库文件进行加密，然后再将其压缩成一个加密的压缩文件。

（6）在命令提示符下使用命令在D盘创建一个名为ABC的文件夹，然后将其深度隐藏。



☑ 想知道数据是怎样进行存储的吗？

☑ 想知道如何恢复硬盘丢失的数据吗？

☑ 想知道如何备份重要的数据吗？

☑ 想知道如何让数据恢复到从前吗？



第 09 章 数据备份防患于未然

今天娜娜很郁闷，因为她竟然糊里糊涂地将电脑中的数据全部清理掉了。娜娜很发愁，不知道该怎么向领导交代，要知道电脑中的资料可关系着她这段时间的成果。阿伟从外面回来，看见娜娜愁眉不展的样子，就问她怎么回事。待娜娜讲完事情的经过，阿伟笑着对她说："没关系，我有办法帮你恢复这些数据！"娜娜听了阿伟的话，仿佛抓到了救命稻草一样，赶紧催促着阿伟为她讲解。

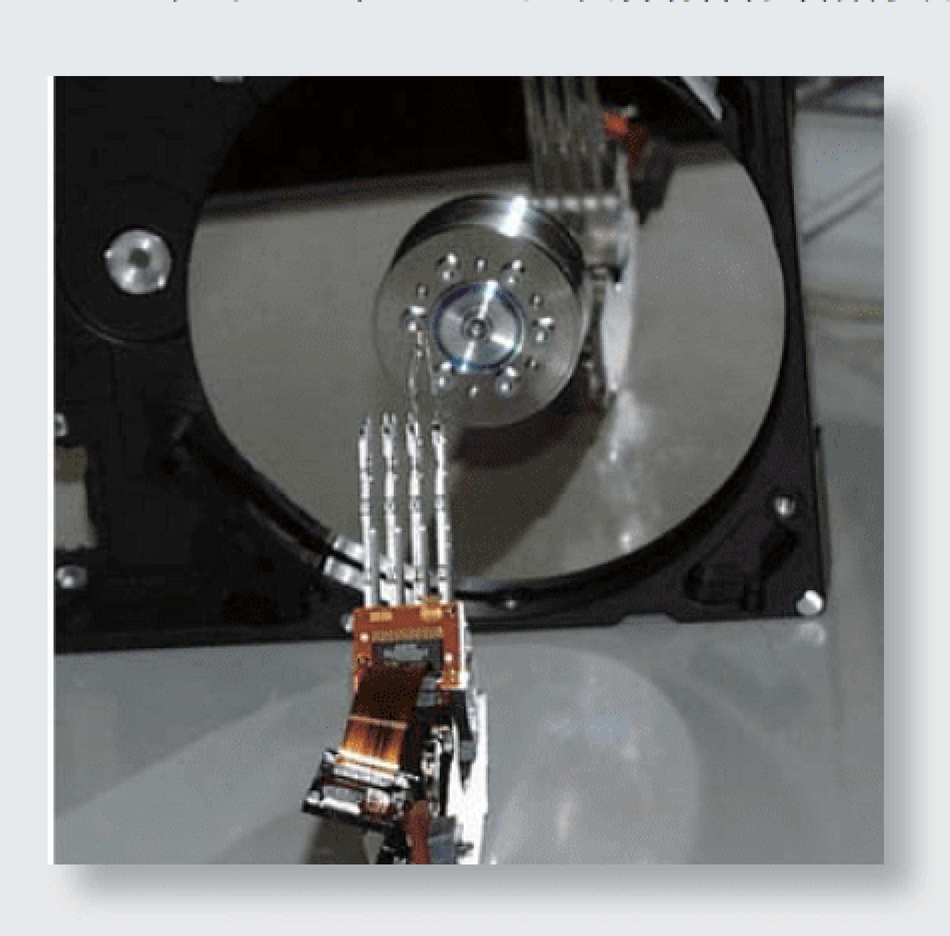
9.1 文件储存原理

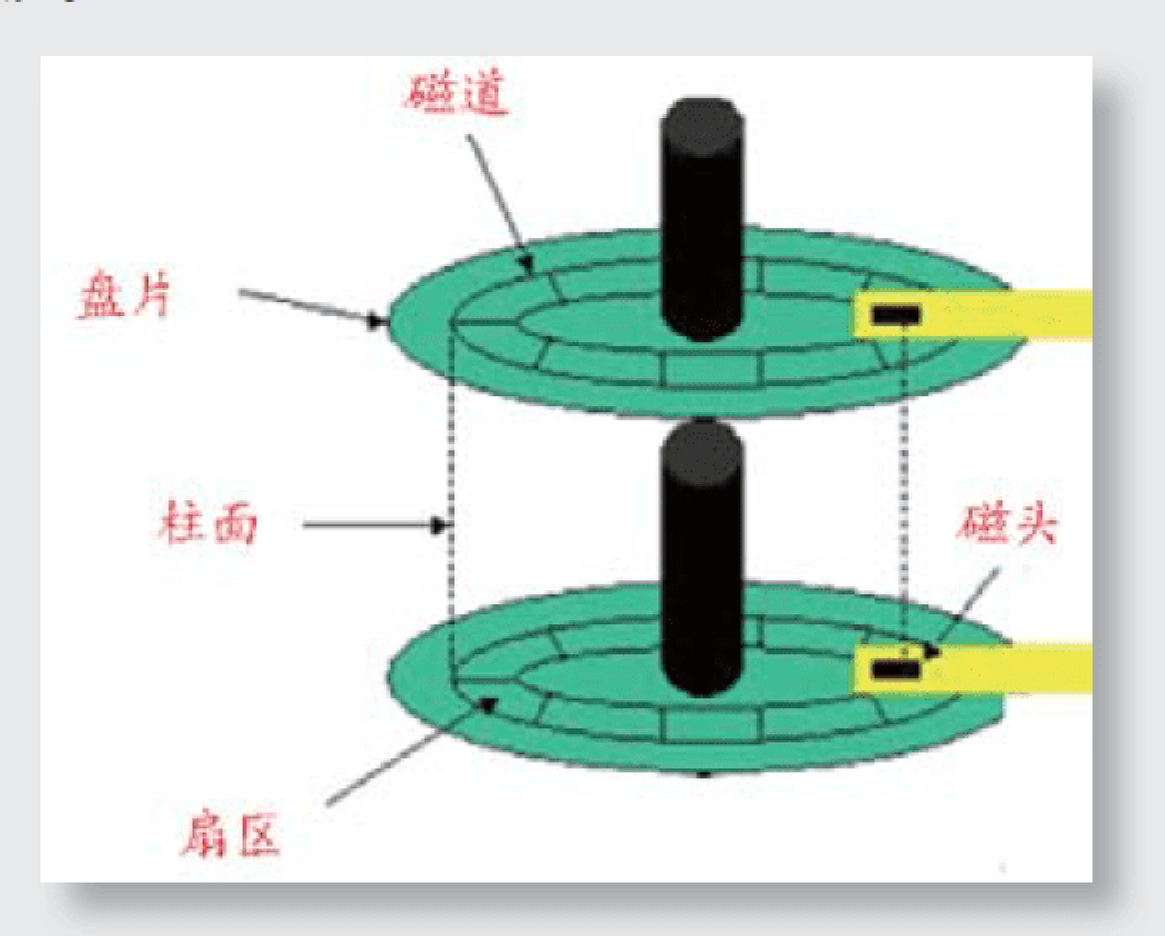
阿伟告诉娜娜："文件其实是按一定规律存储在硬盘中的，了解了这个道理，再掌握了文件的存储分配原理后，对解决硬盘故障、恢复硬盘数据有很大的帮助。"娜娜听了以后，仍然没有理解阿伟所讲的意思，于是可怜兮兮地说："你还是从最基础的知识开始给我讲起吧！"

新手解惑

Q：硬盘主要由哪些硬件结构组成？

A：硬盘的结构主要包括盘片、磁头、磁面、磁道、柱面和扇区。其中，盘片在硬盘中起着承载数据存储的功能。





9.1.1 硬盘存储数据的主要结构

硬盘是电脑文件系统最重要的存储场所，用户可能都遇到过由于重要参数及文件丢失导致电脑不能启动的问题。要解决数据存储的问题，首先应了解硬盘上数据存储的主要结构以及数据存储原理。



下面将对硬盘数据主要的存储单位进行介绍。

1. 主引导扇区

主引导扇区包括硬盘引导程序和分区表。硬盘每个扇区（包括主引导扇区）所储存的信息量都是512个字节，主引导扇区只占用了其中的446个字节，分区的结束标志即最后两个字节"55 AA"。硬盘分区表包含64个字节，共4个分区表项。每个



分区表项的长度为16个字节，其中包含一个分区的引导标志、系统标志、起始和结尾的柱面号、扇区号、磁头号以及本分区前面的扇区数和本分区所占用的扇区数。其中，引导标志表明此分区是活动分区；系统标志决定了该分区的类型；起始和结尾的柱面号、扇区号、磁头号指明了该分区的起始和终止位置。



Q：主要文件系统类型对应的系统标志分别是什么？

A：常见的系统标志有“06”（FAT16分区）、“0B”（FAT32分区）、“07”（NTFS分区）和“63”（UNIX分区）等。

硬盘分区表项的16个字节分配

字节分配	意义
第1字节	分区的激活标志，表示系统可引导。如是0，则表示为非活动分区
第2字节	该分区起始磁头（HEAD）号
第3字节	该分区起始扇区（Sector）号
第4字节	该分区起始的柱面（Cylinder）号
第5字节	该分区系统类型标志
第6~8字节	该分区终止磁头（HEAD）号、分区结束的扇区号、分区结束的柱面号
第9~12字节	该分区首扇区的相对扇区号
第13~16字节	该分区占用的扇区总数

2. 文件分配表

文件分配表是DOS、Windows操作系统的文件寻址格式，常见的文件分配表有FAT16（支持Windows XP操作系统）、FAT32（支持Windows XP操作系统）、NTFS（支持Windows XP/7操作系统）和ext2（支持Linux操作系统）等。文件占用磁盘空间的基本单位是簇，一般情况下，硬盘每簇的扇区数与硬盘的总容量大小有关。同一个文件的数据并不一定完整地存放在磁盘的一个连续区域内，而往往会分成若干段，每一段之间有相互的链接关系。这种存储方式称为文件的链式存储。



Q：实现链式存储的条件是什么？

A：要实现文件的链式存储，在硬盘上必须准确记录已经被文件占用的簇，还必须为每个已经占用的簇指明存储后续内容的下一个簇的簇号。

3. 操作系统引导扇区

操作系统引导扇区是操作系统可直接访问的第一个扇区，它包括一个引导程序和一个被称为BPB的本分区参数记录表。引导程序的主要任务是当主引导扇区将系统控制权交给它时，判断本分区根目录前两个文件是不是操作系统的引导文件。

4. 根目录区

根目录区位于第二个文件分配表之后，记录着根目录下每个文件或目录的起始单元和文件的属性等。操作系统根据根目录区中的起始单元，结合文件分配表就可以知道文件在硬盘中的具体位置和大小。

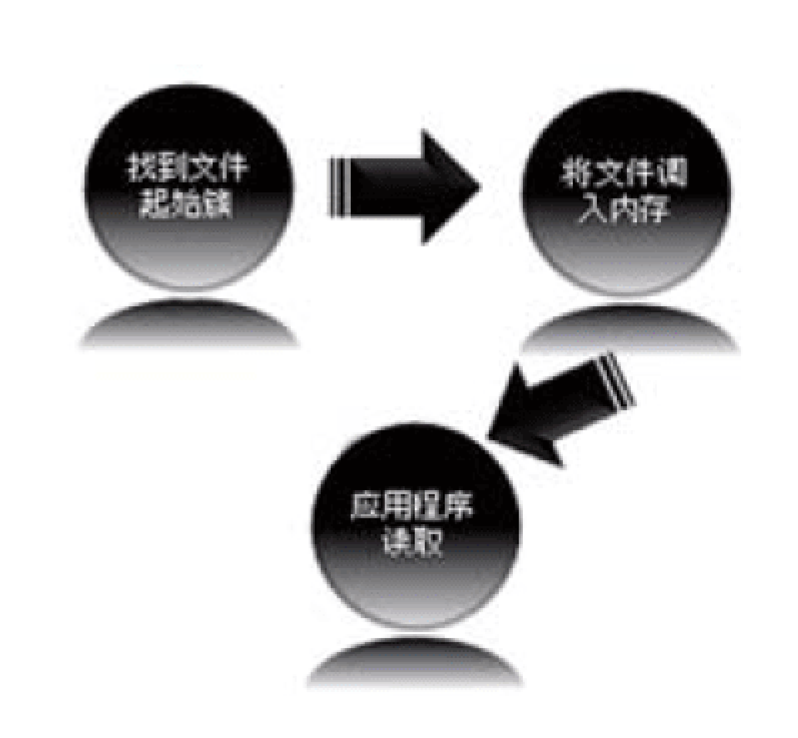
5. 数据区

数据区是真正意义上的存储数据的地方，位于根目录区之后，占据硬盘的大部分空间。硬盘上的数据就存放在数据区。

9.1.2 文件的读取

文件的读取与硬盘的数据区、根目录以及文件分配表有着非常重要的联系，下面将对文件读取的过程进行简单介绍。

硬盘上最重要的数据区除引导区外，还有根目录和文件分配表，根目录中记录了文件及其子目录的属性、尺寸、日期以及它的起始簇，文件分配表里面记录了每个簇的使用分配情况。操作系统读取文件时，先找到根目录区中记录的文件起始簇，明确文件所在的位置，然后再将文件调入到内存中供应用程序使用。





9.1.3 文件的写入

在硬盘中进行文件写入时，会经过一系列过程才能完成，与硬盘的组成密切相关，在整个写入过程中，硬盘的文件分配表起着重要的作用。



下面将对在硬盘中添加新文件所经过的一般过程进行简单介绍。

- **在文件分配表中记录起始簇：** 执行写入操作后，操作系统在根目录中填入文件属性等信息，在文件分配表里面按一定算法找到一个空簇，将其标记占用后，在根目录里面将这个簇作为起始簇记录到其中。
- **形成单链表：** 系统开始将文件内容写入这个簇。如文件没有写完，将会在文件分配表里再找一个空簇，将其标记为占用，并在前一个簇的最后做一个指针指向新的簇，形成一个单链表，然后系统将在这个新的簇里面继续写入内容。
- **写入文件：** 如此重复直到文件内容完全记录完毕。最后系统根据占用的总簇数计算出文件尺寸，并将当前时间写入根目录。

9.1.4 文件的删除

用户在删除一个文件时，系统实际上并没有清除每个簇的内容，只是把根目录里面文件名的首字符换成&符号（其含义是标记这个文件为已删除）；只有当新文件占用了这个簇后，该簇的内容才真正被删除。所以，在簇未被占用之前，文件是可以被恢复的。

教你一招

文件修改的本质

当改变一个文件的属性或名字时，实际上系统只是在根目录里面做了一点改动而已。

9.2 恢复硬盘数据

娜娜听了阿伟介绍的硬盘相关知识，对硬盘存储数据已经有所了解，对找回自己电脑中丢失的文件也增加了些许信心。她问阿伟：“有什么方法能够找回电脑中丢失的文件吗？”阿伟肯定地点点头，回答道：“当然，下面就为你介绍找回电脑中数据的方法。”

9.2.1 硬盘数据恢复的范畴

数据恢复就是把由于遭受到破坏或有硬件缺陷导致不可访问或不可获得的硬盘数据，或由于病毒、误操作和意外事故等各种原因导致丢失的数据还原成正常的数据。数据恢复不仅可以恢复硬盘中的文件，还可以恢复操作系统数据，也可以恢复移动数码存储卡里的数据。



硬盘数据恢复，恢复的是多方面因素造成的数据损坏，下面将分别对其进行介绍。

- **文件丢失：** 主要是误分区、误格式化、系统恢复盘误恢复系统、误删除文件、分区误克隆、分区表信息（MBR）丢失、引导扇区信息（BOOT）丢失、病毒破坏、黑客攻击及恶意程序、磁盘阵列服务器Raid信息丢失、突然断电、内存溢出、软件冲突、强行关机以及死机等情况引起的数据丢失。
- **文件损坏：** Office文档损坏，Microsoft SQL、Oracle、Sybase、Foxbase/pro等数据库文件损坏，图片、ZIP、MPEG、ASF、RM文件损坏，及MS Outlook、Exchange等邮件文件损坏。
- **密码丢失：** 操作系统密码丢失以及ZIP、RAR、Word、Excel、Access和PDF等文档的密码丢失。

9.2.2 使用FinalData恢复文件

恢复硬盘上的数据，可以通过数据恢复软件来完成。这里主要对FinalData进行介绍，FinalData是一款优秀的数据恢复软件，它不仅可以恢复操作系统中被误删除的文件，还可以恢复被误格式化的主引导记录、引导扇区和FAT等数据。



1. 使用FinalData找回误删除的文件

使用FinalData能够方便地找回用户误删除的文件，只要用户删除的文件未被覆盖或短时间内删除的文件，就能轻松地找回。

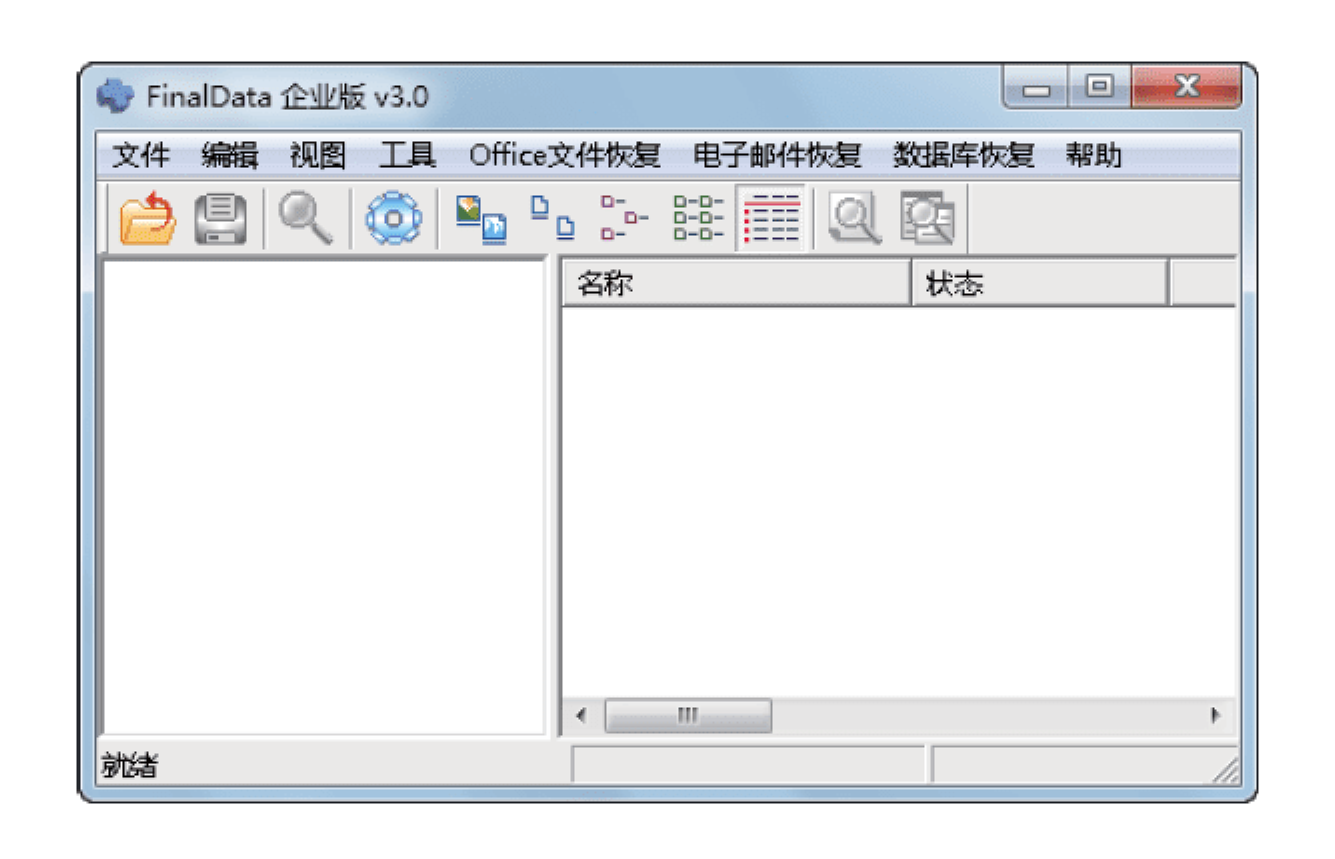


Q：FinalData软件可对任何删除的文件进行恢复吗？

A：FinalData工具并不是万能的，一些删除过久的文件，其数据区有可能已被全部或部分覆盖，这时，软件就无法再恢复它。



下面将以使用FinalData企业版 v3.0（下载地址为http://down.51cto.com/data/77628）为例，介绍在E盘目录下找回误删除的“书目”文件的方法，其具体操作如下。

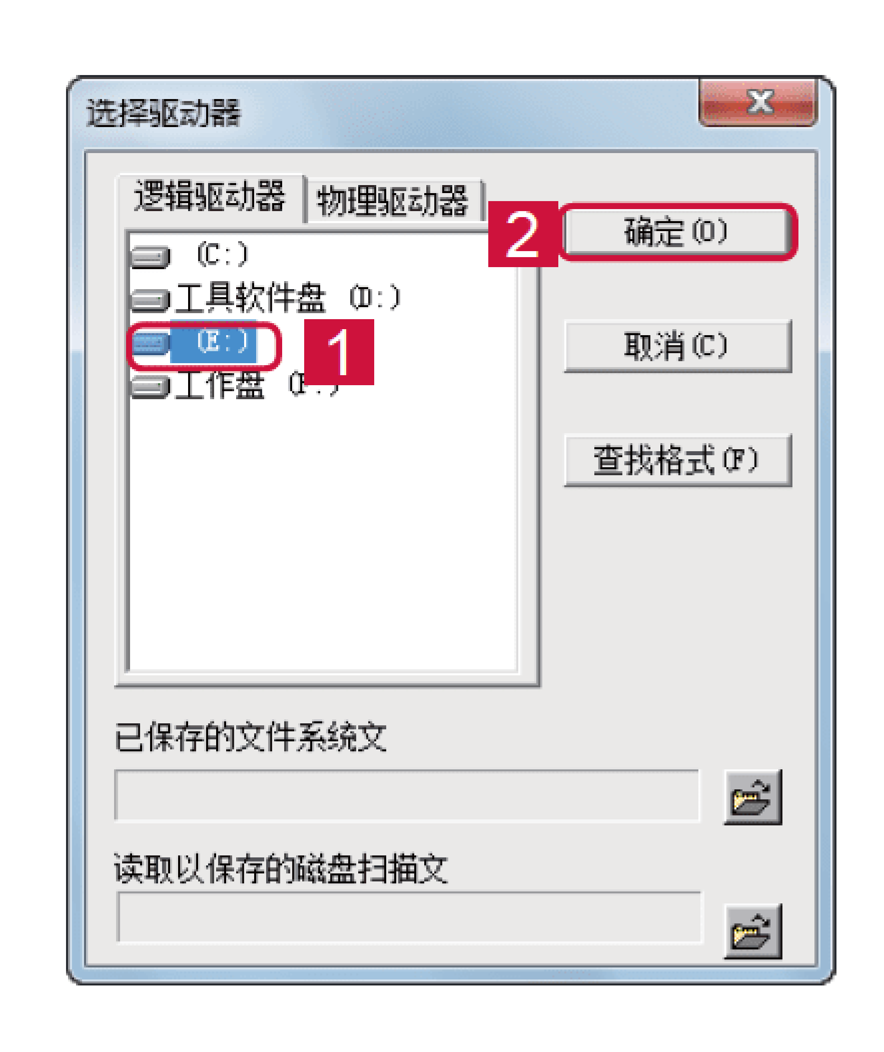


第1步：启动FinalData软件

安装好FinalData 企业版 v3.0后，在桌面上双击该程序的快捷方式图标，运行该软件，在打开的软件主界面中可观察到软件的相关功能选项。

第2步：选择驱动器

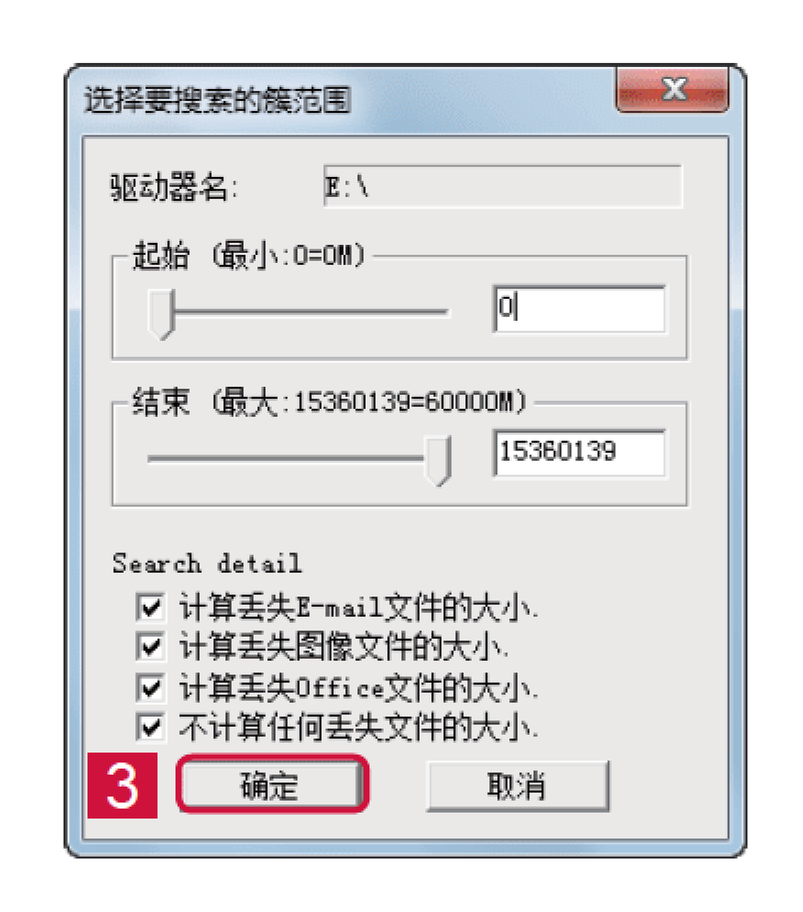
选择“文件”/“打开”命令，在打开的“选择驱动器”对话框中选择“逻辑驱动器”选项卡，在其下的列表框中选择需扫描的驱动器，这里选择（E：）选项，单击 确定(O) 按钮，FinalData将对E盘进行一次初步的扫描。



提示：选择“物理驱动器”选项卡，在其列表框中可选择整个硬盘。

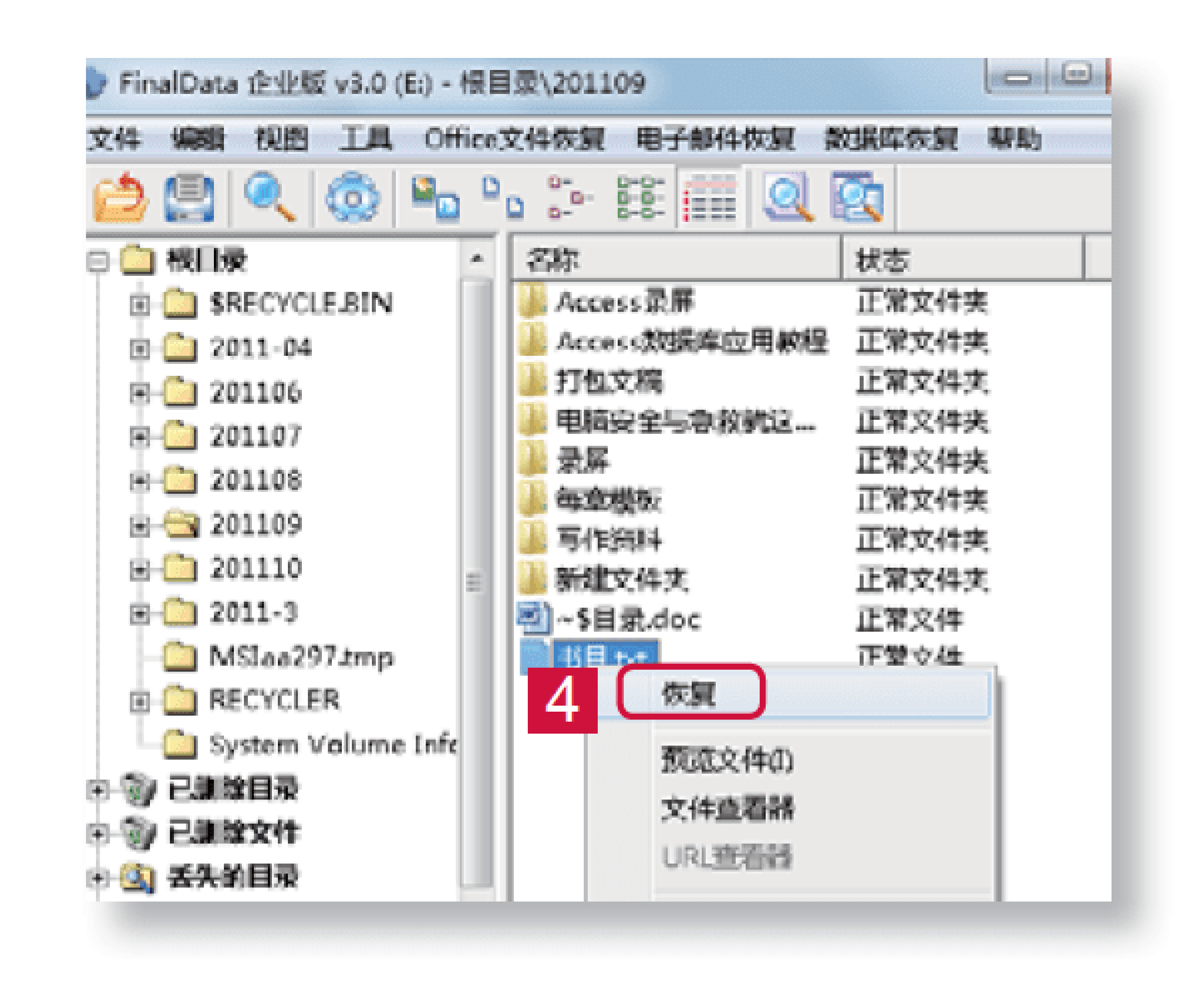
第3步：设置搜索的范围簇

在扫描结束后将打开“选择要搜索的簇范围”对话框，提示要搜索的磁盘簇范围，保持默认设置，单击确定按钮，FinalData将再次对E盘进行全面扫描。



第4步：选择文件进行恢复

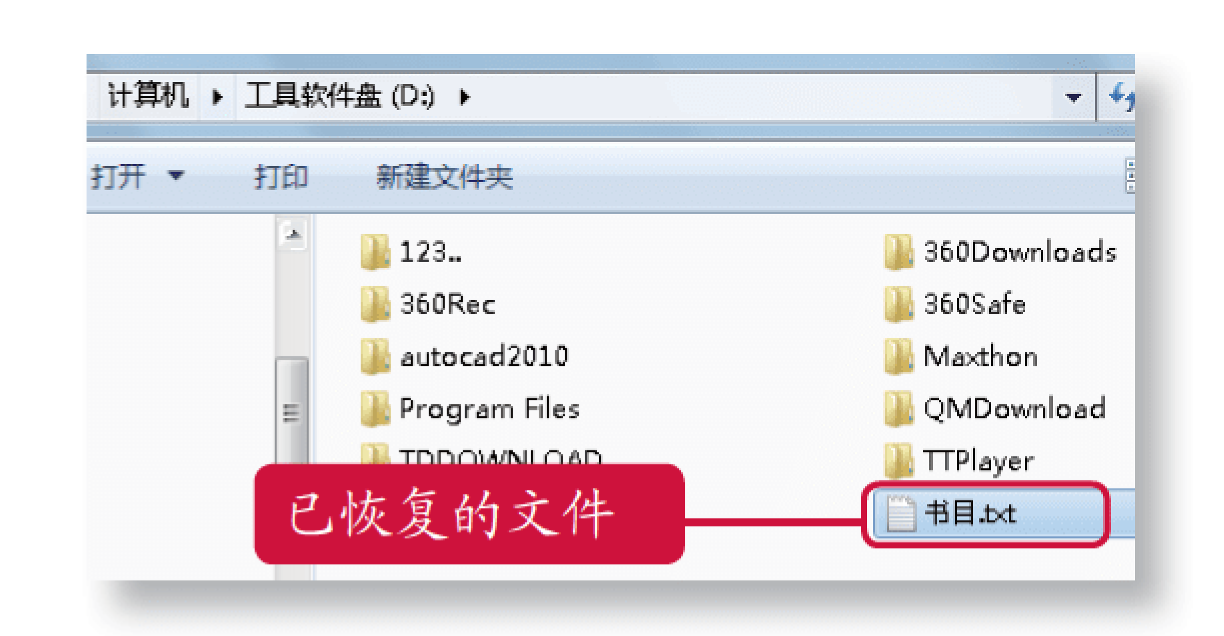
扫描完成后，FinalData将会显示扫描结果，其中列出了E盘中所存在的文件夹，在列出的文件夹中找到需要恢复的文件，在其上单击鼠标右键，在弹出的快捷菜单中选择“恢复”命令。





第5步：选择恢复文件的保存位置

在打开的对话框中选择需恢复文件的保存位置，这里保存到D盘，即选择D:\选项，单击保存按钮，此时FinalData将把“书目”保存在D盘根目录下。



提示：FinalData对中文的长文件名的支持不是很好，如字符长度大于8，恢复的数据将出现乱码。



2. 使用FinalData恢复误格式化分区的文件

使用FinalData恢复误格式化分区的文件和恢复误删除的文件的操作方法相似。当硬盘的分区被格式化之后，只要没再进行过其他操作，硬盘上的数据也是可恢复的，因此，在误格式化分区后，不要再对硬盘进行任何读写操作。



恢复被格式化的分区时需要注意以下几点。

- 恢复的数据以目录形式居多，且目录为中文的长文件名时会出现乱码。
- 并不是该目录内所有的文件都可恢复。
- 如果在格式化分区时加上了参数“u”，将无法恢复该分区下的文件。

9.2.3 使用360文件恢复功能恢复文件

360安全卫士新增了文件恢复功能，可以将删除的文件进行恢复，但需删除文件的位置没有被覆盖才能恢复。



下面将在360安全卫士中启动360文件恢复功能恢复用户误删除的文件，其具体操作如下。



第1步：打开“360文件恢复”窗口

启动360安全卫士，在其主界面中选择“功能大全”选项卡，然后在其中单击“文件恢复”按钮，打开“360文件恢复”窗口。



第2步：扫描文件

在打开窗口的“文件恢复”选项卡的“选择驱动器”下拉列表框中选择“本地磁盘（C：）”选项，然后在其下方单击开始扫描按钮，系统将开始对C盘的删除文件进行扫描并将扫描到的文件显示在其中。

第3步：恢复文件

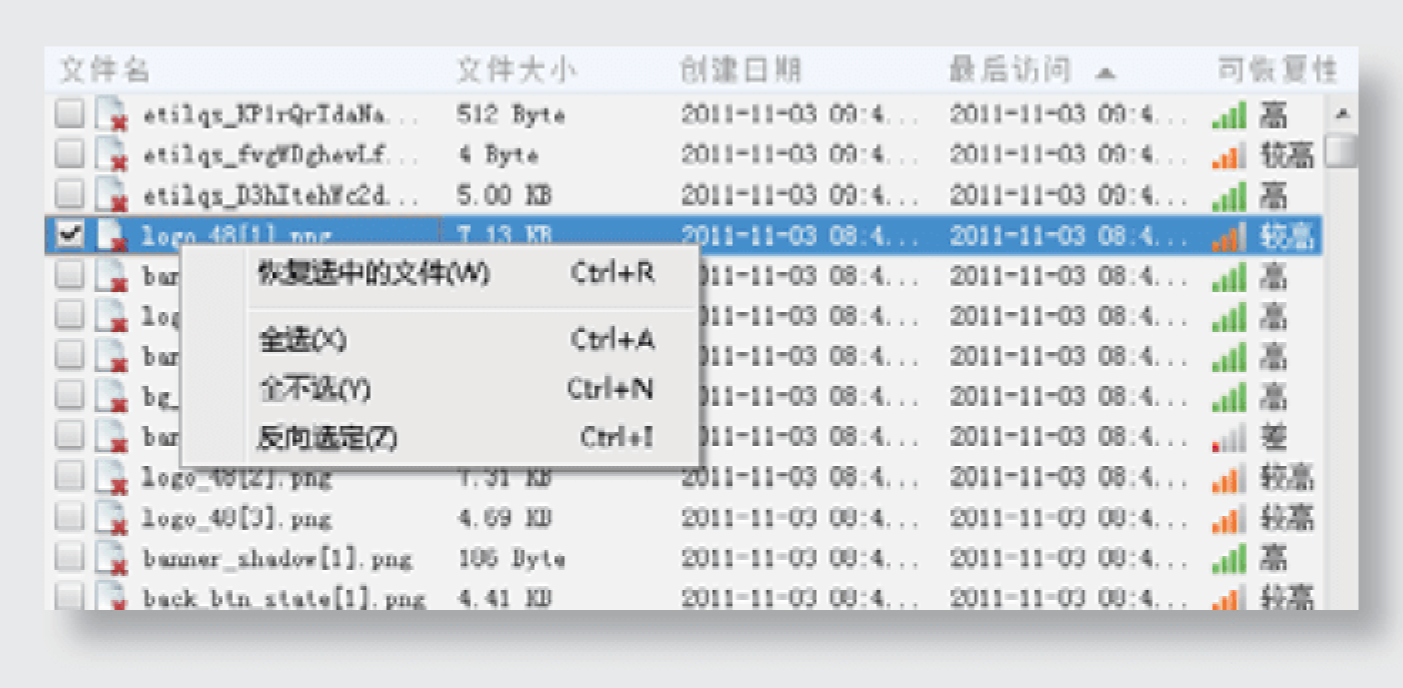
扫描完成后，可选中要恢复的文件前面的复选框，这里单击“全选”超链接，然后单击恢复选中的文件按钮即可恢复选中的文件。



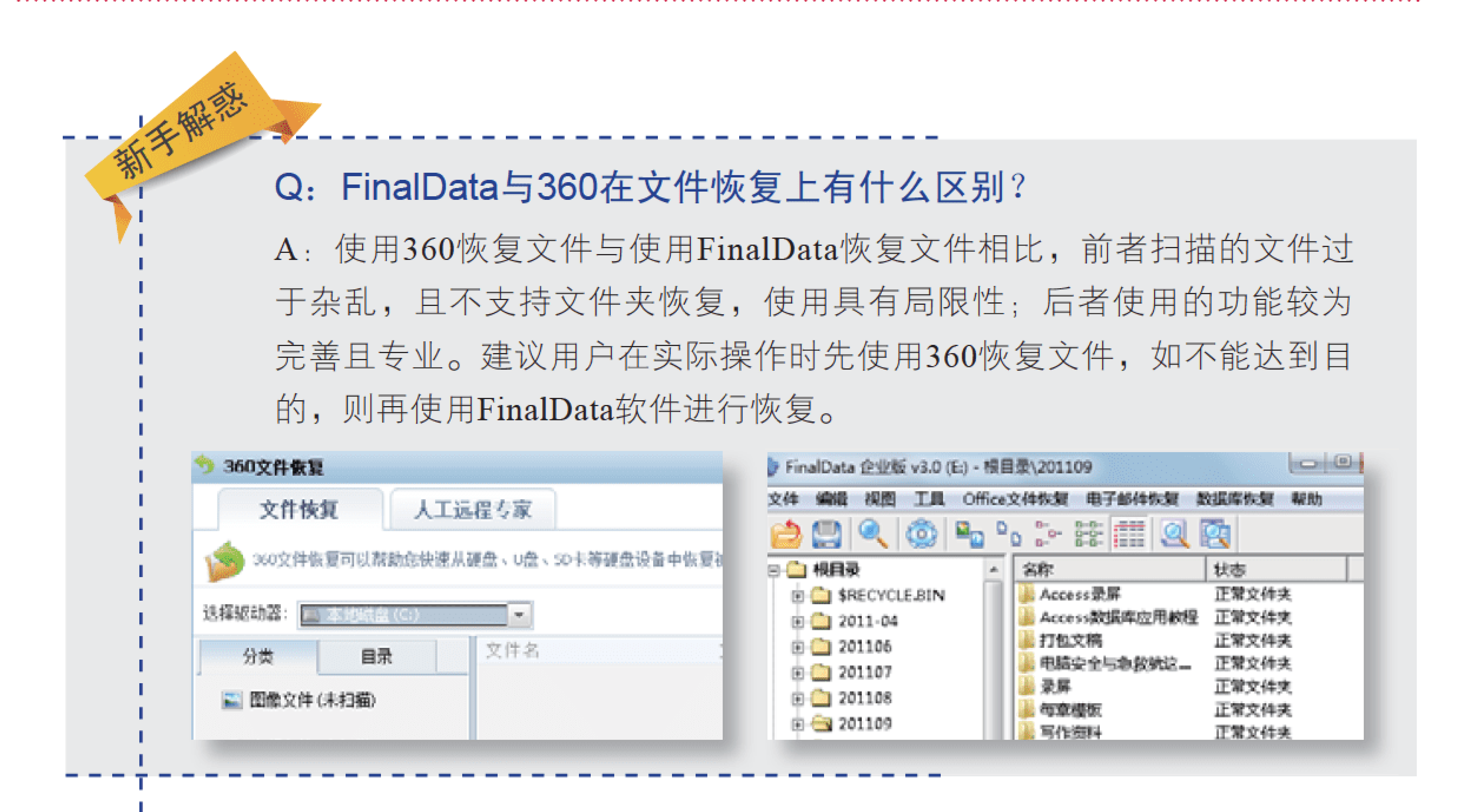
教你一招

使用快捷方式恢复文件

扫描完成后，用户可使用鼠标右键对要恢复文件进行快捷恢复，其方法为：选中要恢复文件前的复选框，然后在其上单击鼠标右键，在弹出的快捷菜单中选择“恢复选中的文件”命令即可。







Q：FinalData与360在文件恢复上有什么区别？

A：使用360恢复文件与使用FinalData恢复文件相比，前者扫描的文件过于杂乱，且不支持文件夹恢复，使用具有局限性；后者使用的功能较为完善且专业。建议用户在实际操作时先使用360恢复文件，如不能达到目的，则再使用FinalData软件进行恢复。

9.2.4 其他的数据恢复软件

目前网络上的数据恢复软件很多，因此，选择一种适合的数据恢复软件非常重要，这样能使用户不再担心电脑中的数据丢失。

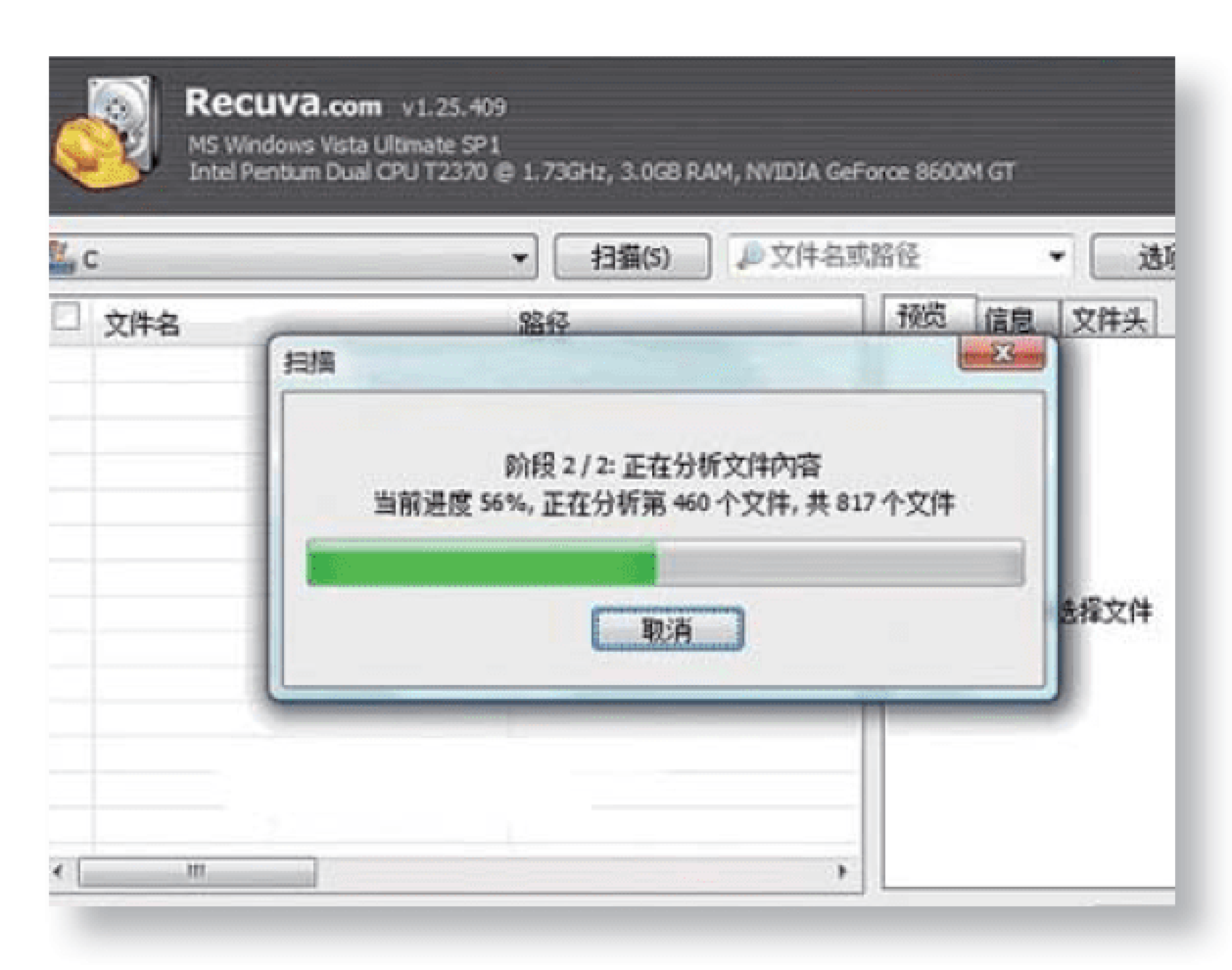


下面将对目前流行的几款数据恢复工具进行简单介绍。

1. EasyRecovery数据恢复软件

EasyRecovery是一款非常强大的硬盘数据恢复工具，能够恢复丢失的数据以及重建文件系统。其通过在内存中重建文件分区表使数据安全地传输到其他驱动器中，可以从被病毒破坏或是已经格式化的硬盘中恢复数据。该软件可以恢复大于8.4GB的硬盘，支持长文件名。丢失的引导记录、BIOS参数数据块、分区表、FAT 表和引导区，都可以由它来进行恢复。





2. Recuva恢复工具

Recuva是一个免费的 Windows 平台下的文件恢复工具，可以用来恢复那些被误删除的任意格式的文件，能直接恢复硬盘、闪盘和存储卡中的文件，只要没被重复写入数据，无论格式化还是删除均可直接恢复，支持FAT12、FAT16、FAT32和NTFS文件系统。新版在向导中添加了iPod的支持，优化了深度扫描和可移动存储驱动器支持。



3. FinalRecovery

FinalRecovery 是一个功能强大而且非常容易使用的数据恢复工具，它可以快速地找回被误删除的文件或文件夹，支持FAT12、FAT16、FAT32和NTFS文件系统，不论文件或者文件夹是在命令行模式中，还是在资源管理器及其他应用程序中删除的，即使已经清空了回收站，它也可以安全并完整地找回来。

4. UndeleteMyFiles

UndeleteMyFiles可以快速简便地找到并恢复已删除的媒介和视频。其操作简单，界面易于使用，扫描速度较快，对于图片、声音、文本和HTML都支持完美恢复。不过因为是国外软件，对于中文文档的恢复能力稍有欠缺，恢复时会出现乱码，但可完美恢复多媒体文件。





9.2.5 特殊情况下损坏数据的恢复

在电脑的使用过程中，经常会遇到由于硬盘的零磁道损坏和分区表损坏而导致的数据丢失现象，这种情况下，需要使用相应的工具软件进行恢复。



下面将对零磁道损坏和分区表损坏的数据恢复方法进行简单介绍。

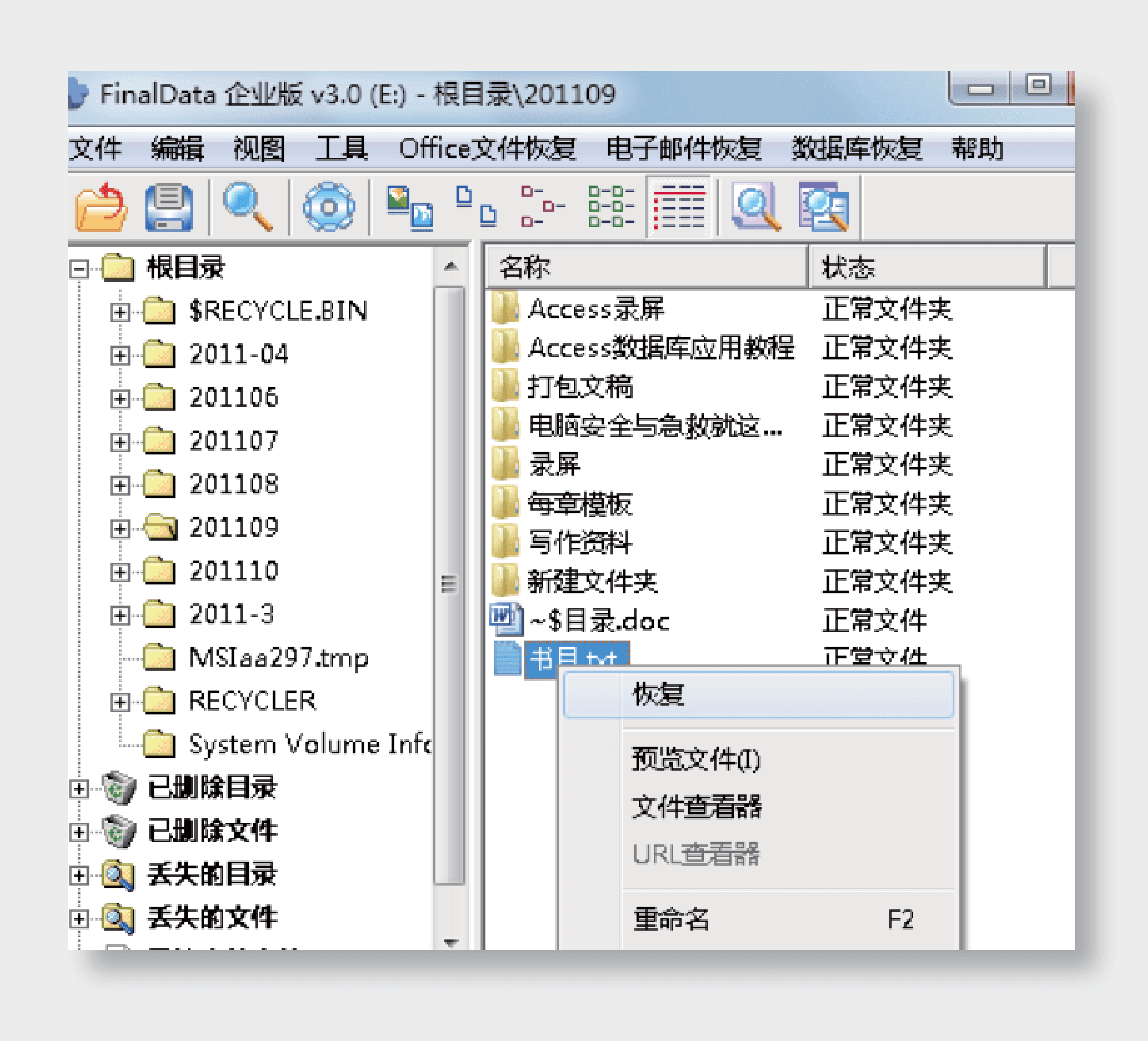
- **零磁道损坏时的数据恢复：** 系统自检能通过，但启动时分区丢失或者C盘目录丢失，硬盘出现有规律的“咯吱……咯吱”的寻道声，运行SCANDISK扫描C盘时，在第一簇出现一个红色的“B”，或者Fdisk找不到硬盘，此种情况即为零磁道损坏。零磁道一旦受损，硬盘的主引导程序和分区表信息将遭到严重破坏，从而导致硬盘无法引导。通常，零磁道损坏的硬盘可以通过PCTOOLS的DE磁盘编辑器（或者DiskMan）来使零磁道偏转一个扇区，使用1磁道作为零磁道来继续使用，而数据可以通过EasyRecovery来按照簇进行恢复。
- **分区表损坏时的数据修复：** 分区表的损坏是分区数据被破坏而使记录被破坏的，可以使用软件来进行修复。在恢复分区上，使用诺顿磁盘医生NDD工具可以自动修复分区丢失等情况，抢救软盘坏区中的数据，强制读出后将其搬移到其他空白扇区。在硬盘崩溃或异常的情况下，NDD可以带给用户一线希望。运行NDD，选择Diagnose进行诊断，NDD会对硬盘进行全面扫描，如果出现错误，它会及时提示，然后只要根据软件的提示选择修复项目即可。
- **误格式化硬盘数据时的数据恢复：** 在DOS高版本状态下，Format格式化操作在默认状态下都建立了用于恢复格式化的磁盘信息，实际上是把磁盘的DOS引导扇区、FAT分区表及目录表的所有内容复制到磁盘的最后几个扇区中，而数据区中的内容没有改变。DOS有一个UnFormat命令，它可以恢复由Format命令清除的磁盘。如果用户在DOS下使用Format命令误格式化了某个分区，可使用该命令恢复。不过UnFormat只能恢复本地硬盘，而不能恢复网络驱动器。使用它还能重新修复和建立硬盘驱动器损坏的分区表。除此之外，还可以使用多种恢复软件来进行数据恢复，如EasyRecovery和FinalData等恢复软件均可以很方便地进行数据恢复工作。



跟我练习

使用FinalData软件扫描近期删除的文件，并恢复重要的文件

启动FinalData软件，然后选择“文件”/“打开”命令，在打开的“选择驱动器”对话框的“逻辑驱动器”列表框中选择需扫描的驱动器，根据提示进行操作，待扫描出删除的文件后，将重要的文件进行恢复。



9.3 备份和恢复重要数据

阿伟告诉娜娜，通常情况下，应该对操作系统中的重要数据进行备份。娜娜疑惑地看着阿伟，问：“那什么是数据备份呢，怎样进行备份？”阿伟很惊讶，他没想到娜娜连数据备份都不知道，于是对她说：“不用着急，我现在就为你好好地补充一下这方面的知识，并教你怎样通过备份文件进行恢复。”

9.3.1 备份和还原注册表

注册表是黑客经常攻击的对象，用户需要对其进行备份，这样当出现问题时便可及时还原，以防止注册表被攻击导致不可估量的严重后果。



1. 备份注册表

Windows优化大师（下载地址为http://xiazai.zol.com.cn/detail/36/355554.shtml）是一款功能强大的系统辅助软件，它提供了全面有效且简便安全的系统功能选项，用户可使用它方便快捷地对注册表进行备份。



下面将使用Windows 7优化大师备份注册表，其具体操作如下。



第1步：选择“系统清理”选项卡

在电脑中安装Windows 7优化大师v1.06正式版，然后在桌面上双击其快捷方式启动软件，在打开的主界面中选择“系统清理”选项卡，打开系统清理大师界面。

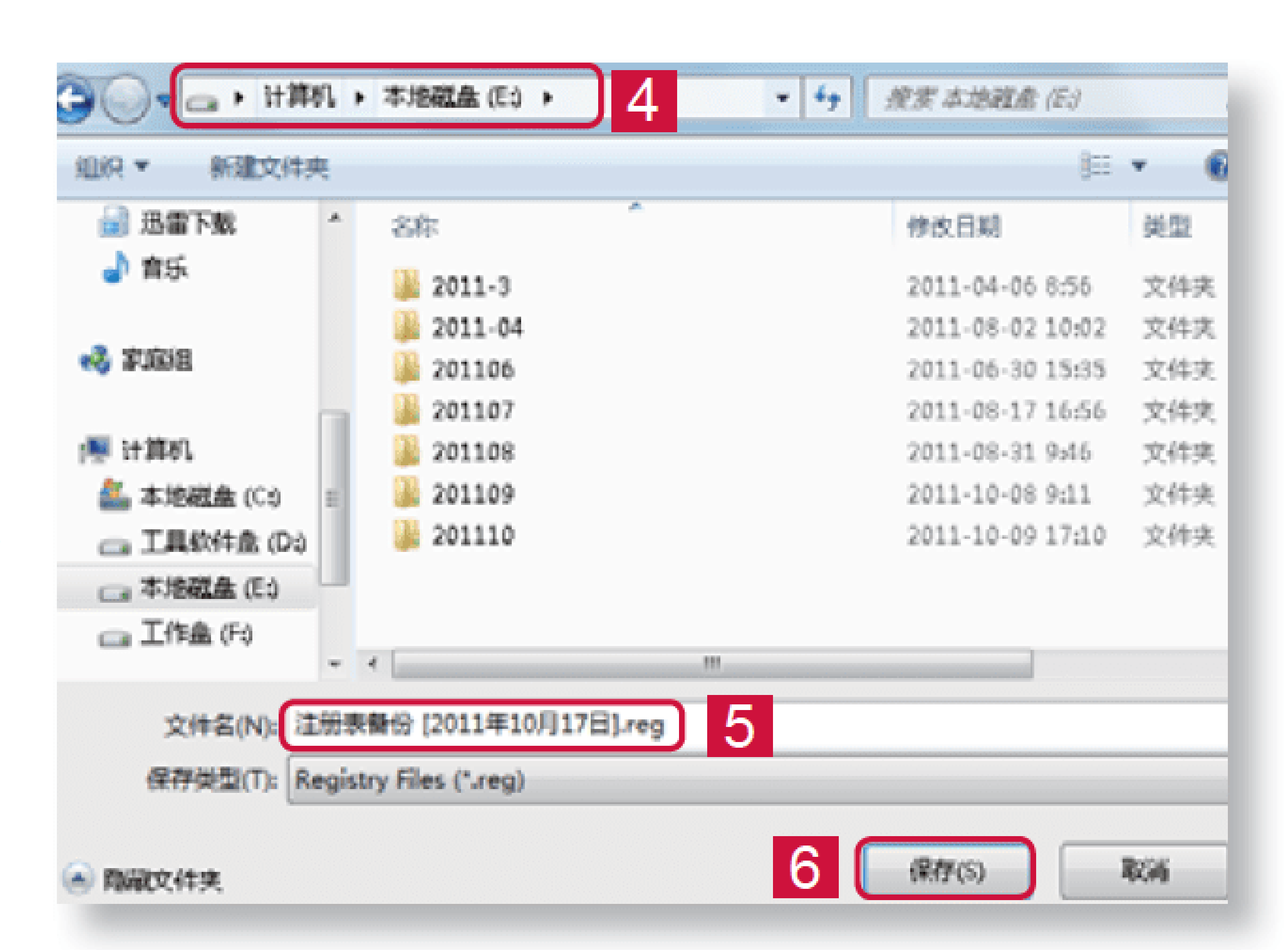


第2步：选择备份整个注册表

在打开的界面中单击“注册表清理”超链接，在其右侧单击备份整个注册表按钮对整个注册表进行备份。

第3步：选择备份位置

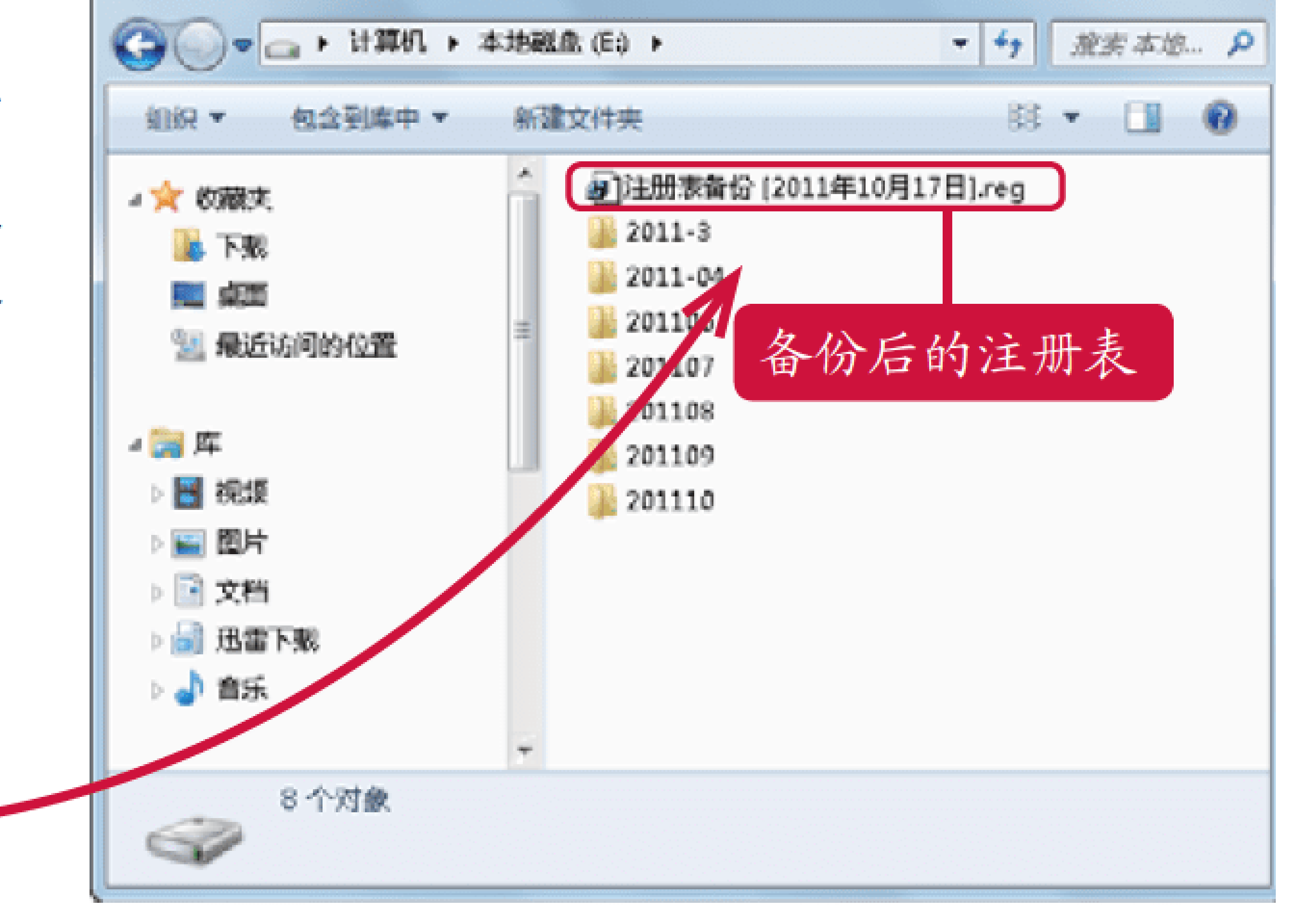
在打开的“注册表备份”对话框上方的下拉列表框中选择备份文件要保存的位置，这里选择E盘，在下方的“文件名”文本框中输入要保存的文件名，这里保持默认，然后单击保存(S)按钮即可开始备份。



第4步：完成备份

完成备份后，系统将打开提示对话框提示备份完成，单击确定按钮关闭即可，此时打开相应的保存路径即可查看备份文件。





2. 还原注册表

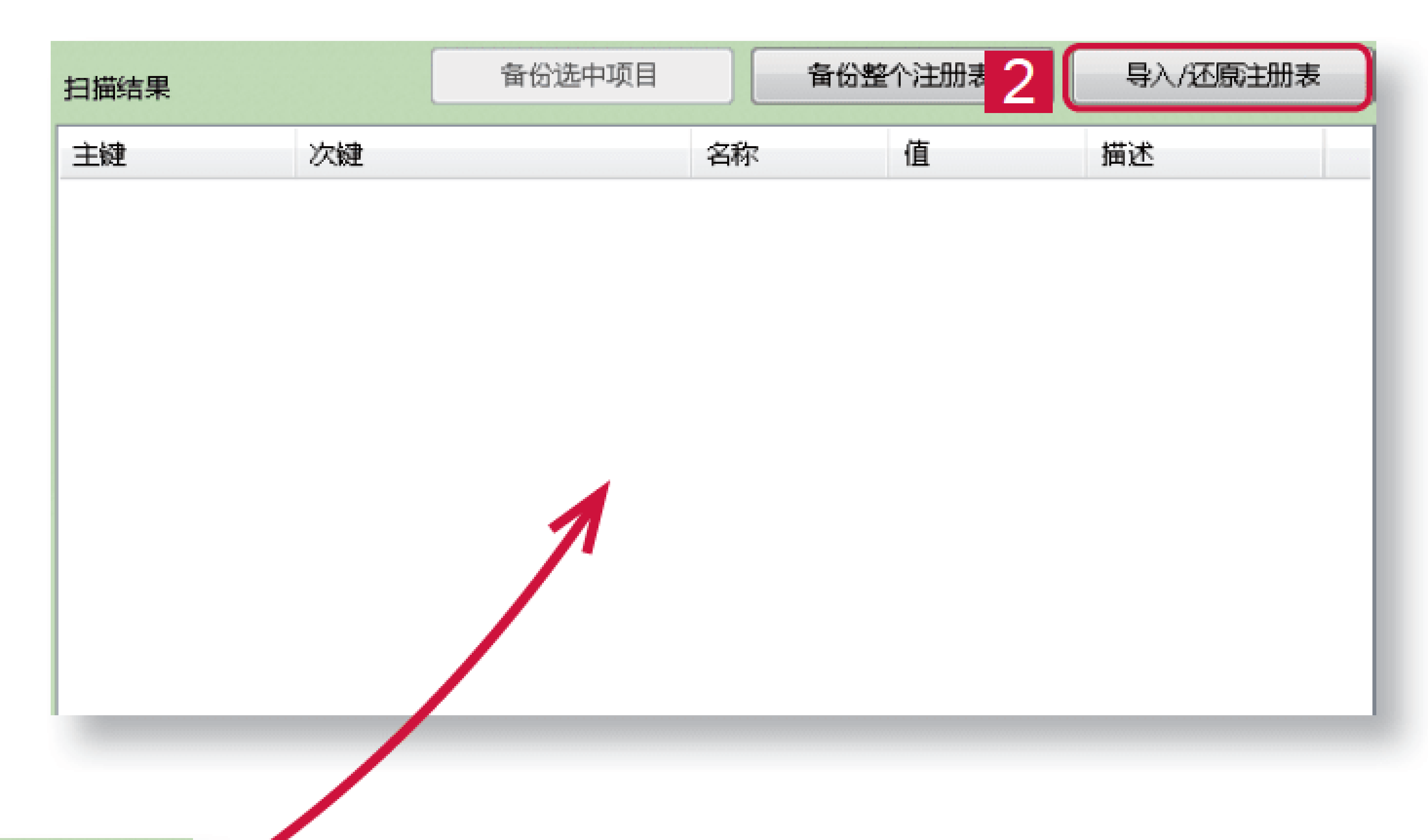
当注册表被破坏或出错时，需要对其进行恢复，这时同样可使用Windows 7优化大师实现。



下面将使用Windows 7优化大师还原注册表，其具体操作如下。

第1步：选择还原选项

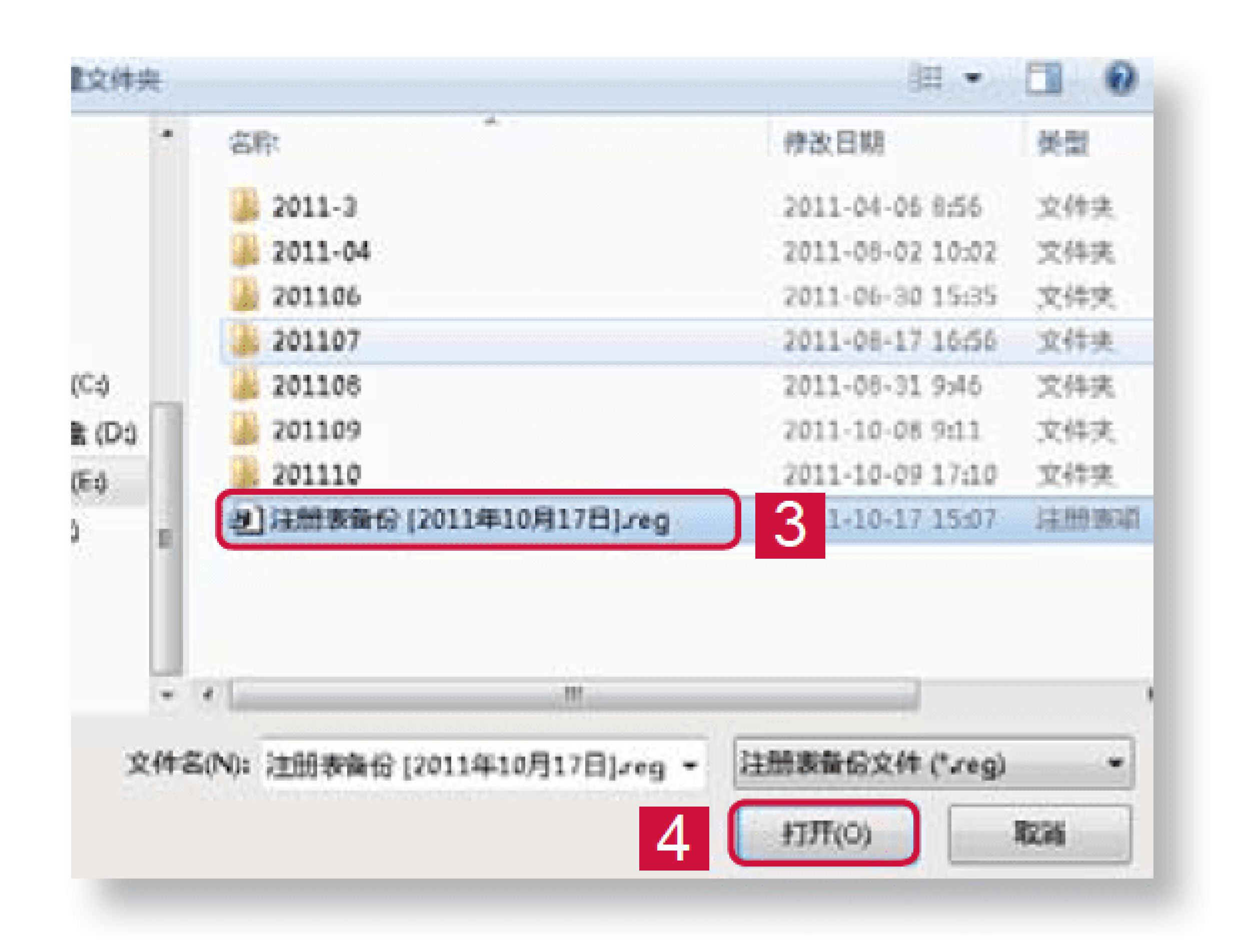
启动Windows 7优化大师，打开系统清理大师界面，单击“注册表清理”超链接后，单击导入/还原注册表按钮，打开restore对话框。





提示：可对注册表中的垃圾文件进行清理后再进行驱动程序的还原，以确保恢复注册表的安全性。





第2步：选择备份文件

在打开的对话框中找到相应的注册表备份文件，选择该文件，然后单击打开(O)按钮，系统将开始还原。

提示：还原完成后，系统将打开提示对话框提示还原完成，然后单击确定按钮。

9.3.2 备份和还原驱动程序

驱动精灵（下载地址为http://dl.pconline.com.cn/download/64945.html）是一款集驱动管理和硬件检测于一体的专业管理工具，为用户提供驱动备份和恢复等实用功能，并有多国语言界面供用户选择，用户在重装系统前可使用其对驱动程序进行备份，以节约安装时间。

1. 备份驱动程序

手动备份驱动程序十分费时，因此最好使用专业的工具进行备份，使用驱动精灵能快速地为电脑中的驱动程序进行备份。



下面将使用驱动精灵2011备份电脑的驱动程序，其具体操作如下。



第1步：选择要备份的驱动

启动驱动精灵2011，在其主界面中单击“驱动管理”按钮，在其下方选择“驱动备份”选项卡，然后选中要备份的驱动程序选项前的复选框，单击“我要改变备份设置”超链接，打开“系统设置”对话框。



第2步：设置备份选项

在打开的对话框中选择“驱动程序”选项卡，在其右侧“驱动备份路径”文本框中设置备份的位置，在“备份设置”栏中选中“备份驱动到文件夹”单选按钮，然后单击 确定(A) 按钮返回备份界面。

第3步：备份驱动程序

单击 开始备份 按钮，系统开始备份驱动程序，并显示备份进度。



提示：由于前面选择的是“备份驱动到文件夹”，因此备份完成后，驱动程序将以文件夹的形式进行保存。

2. 还原驱动程序

使用驱动精灵不仅能快速地进行备份，而且还能在重装系统后快速地使用备份文件进行还原。



下面将使用驱动精灵对驱动程序进行还原，其具体操作如下。



第1步：打开还原窗口

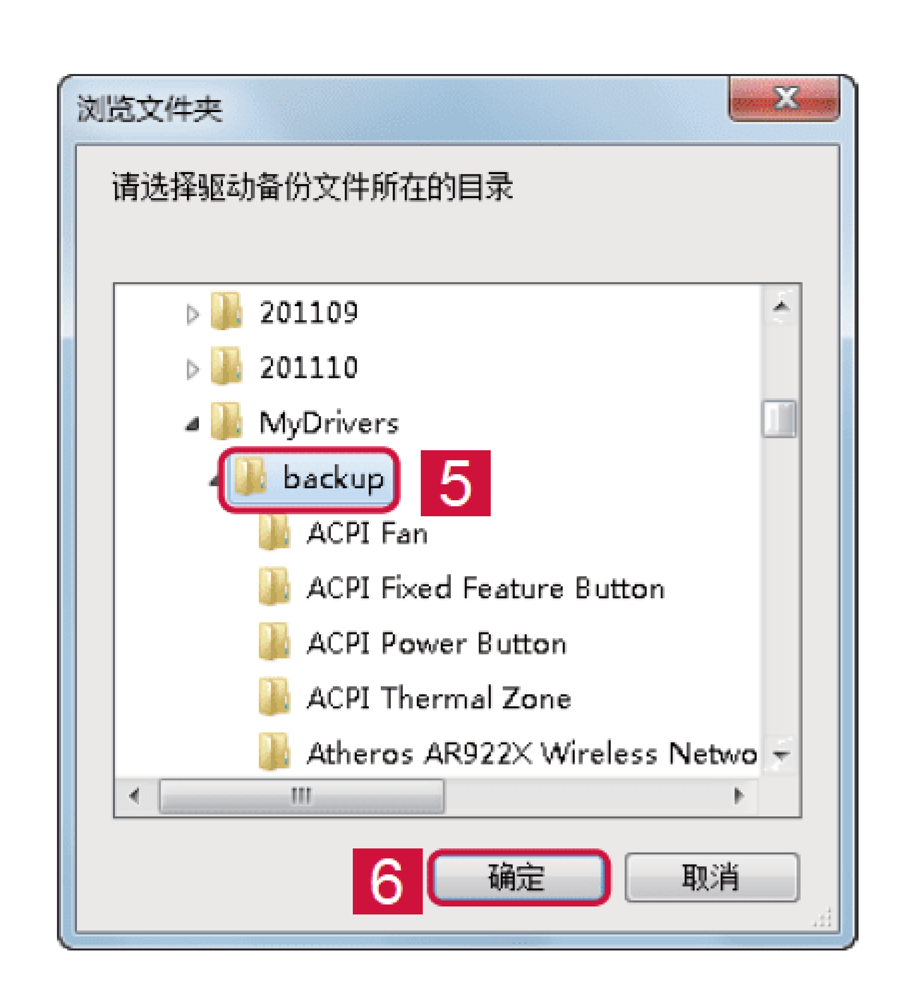
启动驱动精灵，在其中单击“驱动管理”按钮，选择“驱动还原”选项卡，在其下方右侧的“备份模式”下拉列表框中选择“文件夹”选项，然后单击 按钮。





第2步：选择备份文件夹

在打开的“浏览文件夹”对话框的下拉列表框中选择备份的驱动程序文件夹，然后单击确定按钮，将备份文件列表添加到驱动精灵对话框左侧列表框中。



教你一招

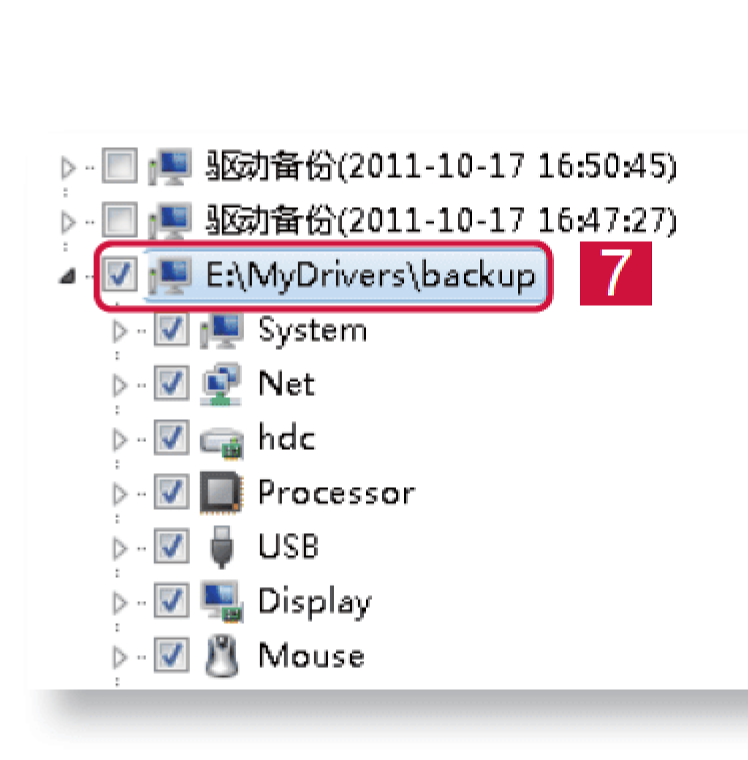
选择还原相应的驱动程序

在“浏览文件夹”对话框中找到备份的驱动程序文件，然后在其中选择相应的硬件驱动程序即可还原选择的驱动程序，而不必还原整个备份。

第3步：还原驱动程序

返回还原驱动程序窗口，在其左侧选中添加的备份文件前的复选框，然后单击右侧的开始还原按钮，即可打开“正在安装驱动程序”对话框，根据向导依次进行操作即可完成驱动程序的还原。





9.3.3 备份和恢复文件

Windows 7操作系统具有文件的备份和还原功能，利用该功能可以将用户的文件备份到指定的硬盘或分区中，同时，也可利用备份的文件将数据恢复到指定的位置，该功能非常方便，用户的使用不会影响备份的操作。

1. 备份文件

首次打开备份工具时，用户需要先对备份进行设置，即在打开的向导中设置备份的存储位置和备份对象等。



下面在Windows 7中利用文件和设置备份功能将F盘中的“光盘”文件夹备份到E盘中，其具体操作如下。



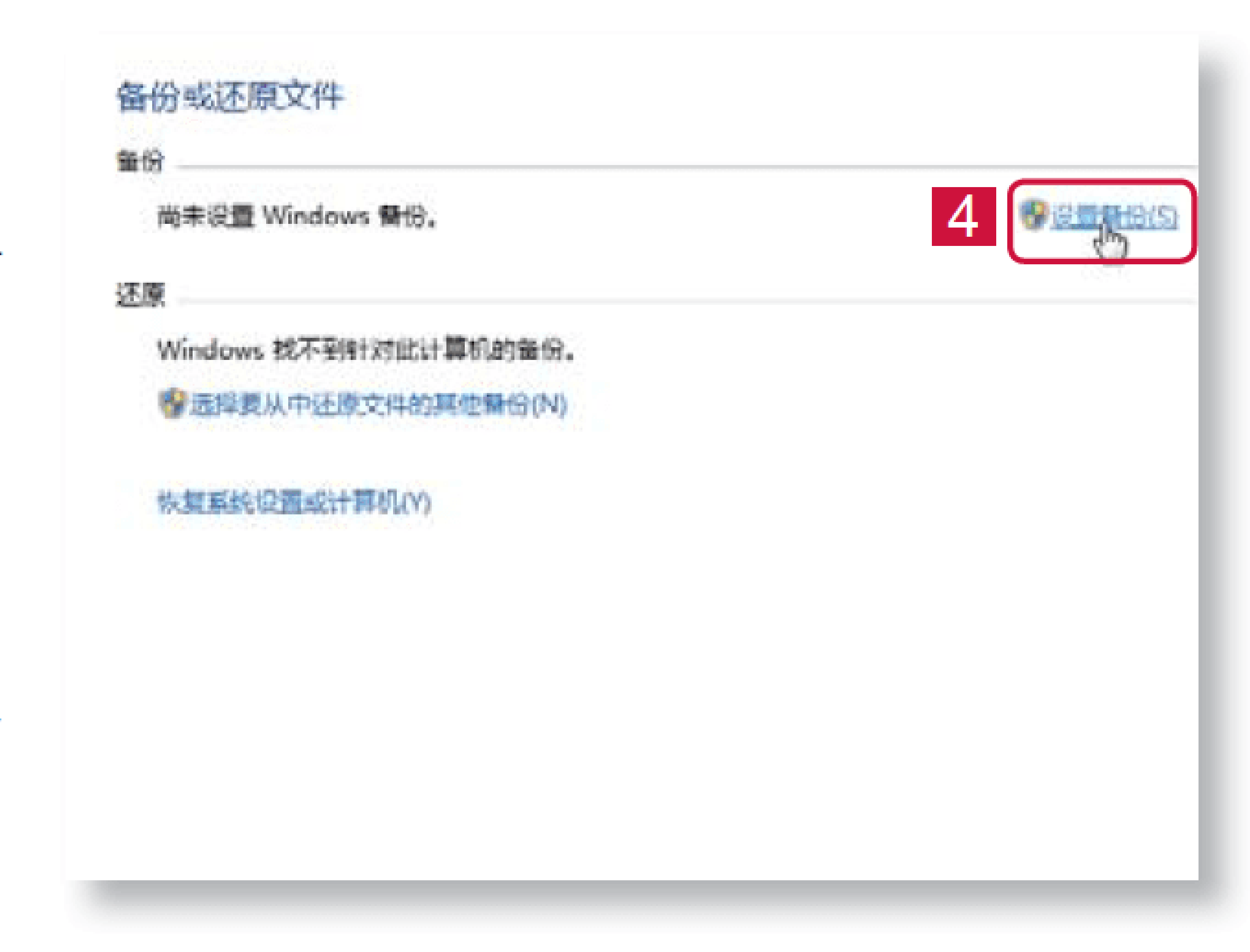
第1步：打开备份窗口

单击“开始”按钮，在“搜索程序和文件”文本框中输入“backup”，在其列表中将出现与之相关的列表项，这里选择“备份您的计算机”选项，打开备份窗口。

第2步：打开备份设置对话框

在打开的“备份或还原文件”对话框中单击“设置备份”超链接，即可进行备份选项的相关设置。

提示：由于是第一次进行备份，因此，在对话框中出现尚未设置Windows备份的提示信息。





第3步：设置保存位置

在打开的“选择要保存备份的位置”对话框的“保存备份的位置”列表框中选择“本地磁盘（E：）”选项，然后单击下一步(N)按钮。

提示：单击保存在网络上(V)...按钮，可在打开的对话框中设置将备份保存在局域网的共享文件夹中。



新手解惑

Q：备份位置该怎么选择呢？

A：使用Windows自带的备份功能时，备份的位置只能是驱动器，而不能是具体的文件夹。



第4步：设置备份内容类型

在打开的“您希望备份哪些内容？”对话框中选中“让我选择”单选按钮，选择用户希望备份的库或文件夹，然后单击下一步(N)按钮。

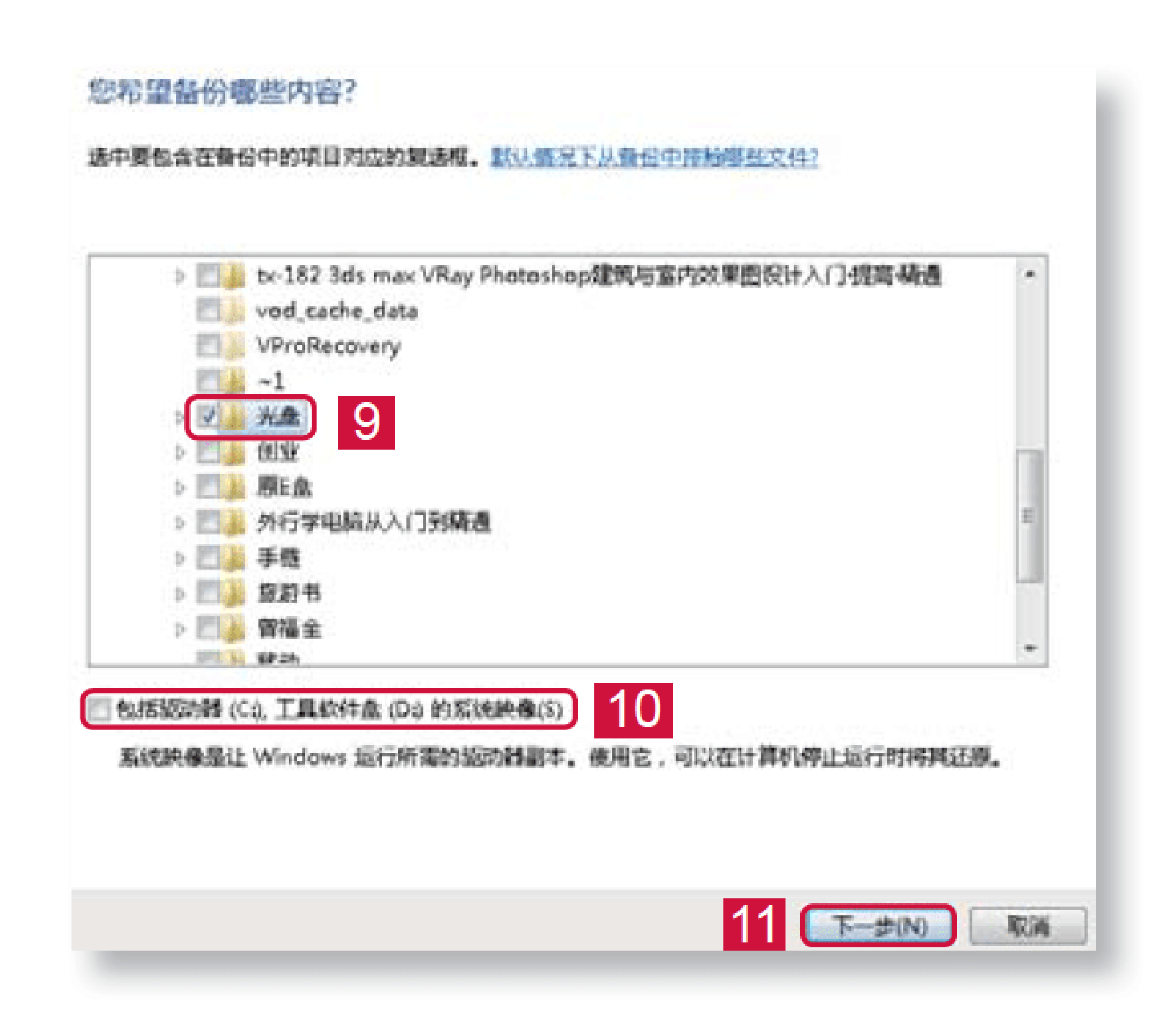
教你一招

使用默认的文件选择功能

在该对话框中选中“让Windows选择”单选按钮，系统将全面地创建Windows相关重要资料的备份。

第5步：选择备份对象

在打开对话框的下拉列表框中选择要备份的文件，这里选择“光盘”选项，取消选中“包括驱动器（C：），工具软件盘（D：）的系统映像（S）”复选框，然后单击下一步(N)按钮。



第6步：确认并保存备份设置

在打开的“查看备份设置”对话框中核对备份的设置，确认无误后，单击保存设置并退出(S)按钮完成备份设置。

提示：在此对话框中单击“更改计划”超链接，可在打开的对话框中对进行备份的频率和时间进行设置。



第7步：开始备份

在打开的对话框中显示系统正在进行文件备份，单击查看详细信息(I)按钮可查看文件的备份过程。

提示：如文件较大，不建议使用该方法进行备份，可使用专业的备份软件进行备份。



2. 恢复文件

当文件遭到破坏或被病毒感染丢失时，可以通过备份的数据和相应的恢复操作将其恢复。



下面将使用Windows 7自带的还原功能将备份的文件通过还原向导进行恢复，其具体操作如下。



第1步：进入还原窗口

打开“备份或还原文件”对话框，在其中可查看备份文件的大小以及备份时间，然后单击 还原我的文件(R) 按钮，打开备份设置向导。



第2步：选择备份文件夹

在打开的对话框中单击 浏览文件夹(O) 按钮，即可在打开的“浏览文件的备份”对话框中选择前面备份的文件，然后单击 添加文件夹(O) 按钮。

提示：单击 浏览文件(I) 按钮，在打开的对话框中选择备份中的文件进行添加，而不必添加整个文件夹。



第3步：设置还原路径

返回上一步对话框，单击[下一步(N)]按钮，在打开的对话框中选中“在以下位置”单选按钮，然后单击其文本框右侧的[浏览(W)...]按钮，打开“浏览文件夹”对话框。



提示：在其中选中“在原始位置”单选按钮，系统即可将备份的文件夹还原到原来的位置。

第4步：选择还原位置

在打开的对话框中选择“本地磁盘（E：）”选项，然后单击[确定]按钮即可将文件还原到该位置。



第5步：还原文件

打开“还原文件”对话框，在其中将显示还原文件的进度，还原完成后，系统将提示文件还原成功，然后单击[完成(F)]按钮即可。



新手解惑

Q：常用复制型备份文件的方法与备份功能有什么不同？

A：通常用户使用备份文件的方式是通过将文件复制到移动硬盘中进行存放，与通过系统备份还原功能备份和还原文件的最大区别在于其备份还原速度太慢且占用的存储空间太大。

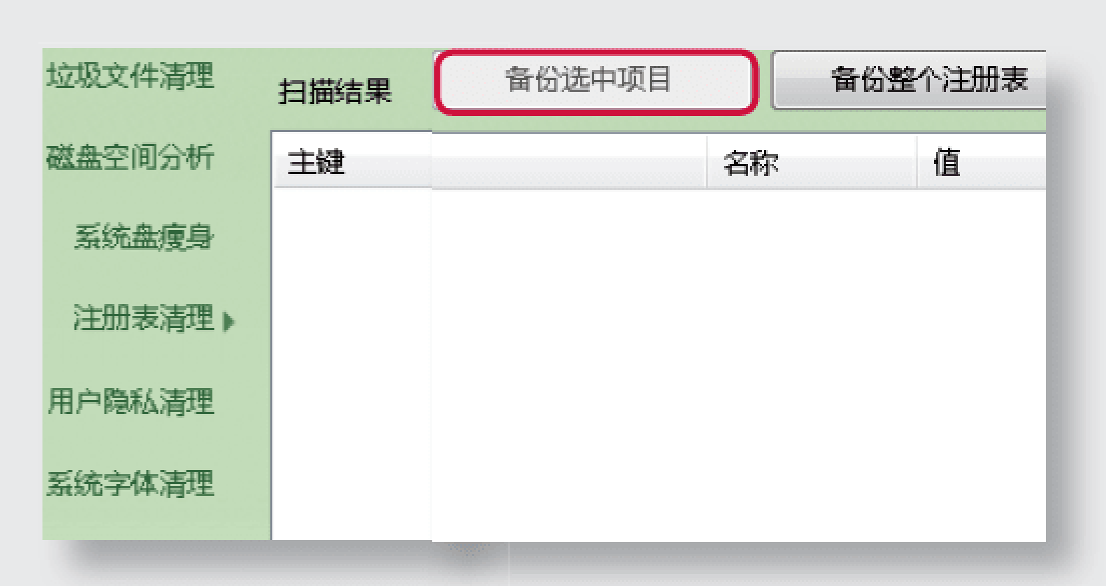
跟我练习

对电脑中的重要数据进行备份，包括注册表、驱动程序以及重要文件

任务1：使用Windows 7优化大师对注册表进行备份，防止因误操作导致的注册表信息被破坏。

任务2：使用驱动精灵2011的驱动管理功能对驱动程序进行备份，重装系统后，可使用其还原驱动程序。

任务3：收集整理电脑中的重要文件，使用系统备份功能对其进行备份。





9.4 更进一步——硬盘数据小妙招

阿伟给娜娜讲解了这些数据备份和恢复的知识后，娜娜已经能很好地掌握。为了使娜娜在实际的使用过程中更快速方便地进行相关的操作，阿伟决定再教给她一些简单的方法，这样，娜娜将不仅能够使用安全的方法为相关数据进行备份，而且还能够在熟练的基础上进行快捷操作。

第1招 创建批处理文件备份注册表

注册表是黑客程序、后门、病毒及恶意网站最常攻击的目标，因此必须对其进行备份，使用批处理的方法能快速地进行注册表的备份，其方法如下。

①创建一个文本文档，在其中输入相关代码，并以“.bat”格式的文件类型进行保存。

②双击保存的批处理文件，系统将自动对注册表进行备份。

```
@echo off
set mypath=“C: myfolder”%date%“”
if exist “%mypath%” rd /s /q “%mypath%”
md “%mypath%”
cd “%mypath%”
reg export hkcu myreg.reg
reg export hklm sysreg.reg
```

教你一招

使用批处理备份注册表

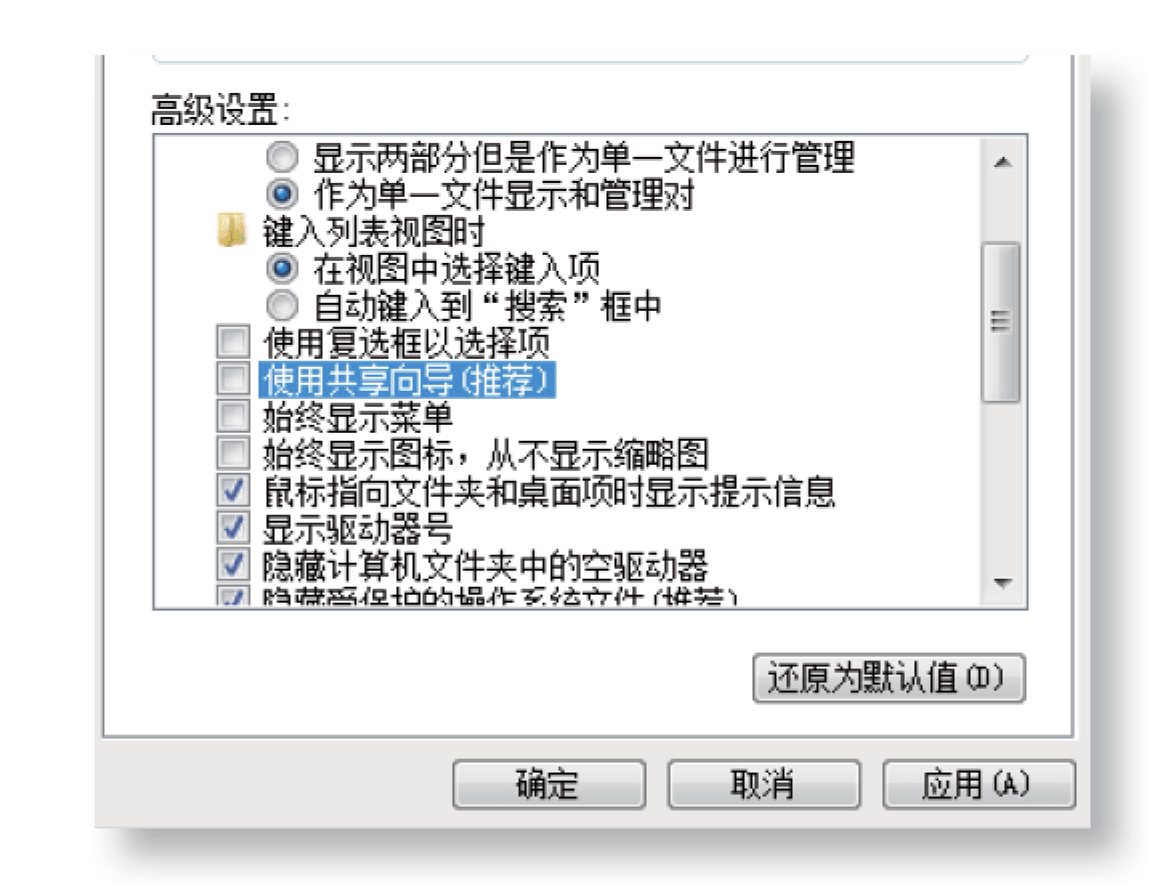
备份注册表的批处理代码是：

```
@echo off
set mypath=“C:myfolder”%date% “”
if exist “%mypath%” rd /s /q “%mypath%”
md “%mypath%”
cd “%mypath%”
reg export hkcu myreg.reg
reg export hklm sysreg.reg
```

该代码表示在电脑C盘中以当前日期名创建一个目录，然后将个人和系统注册表数据导入其中。

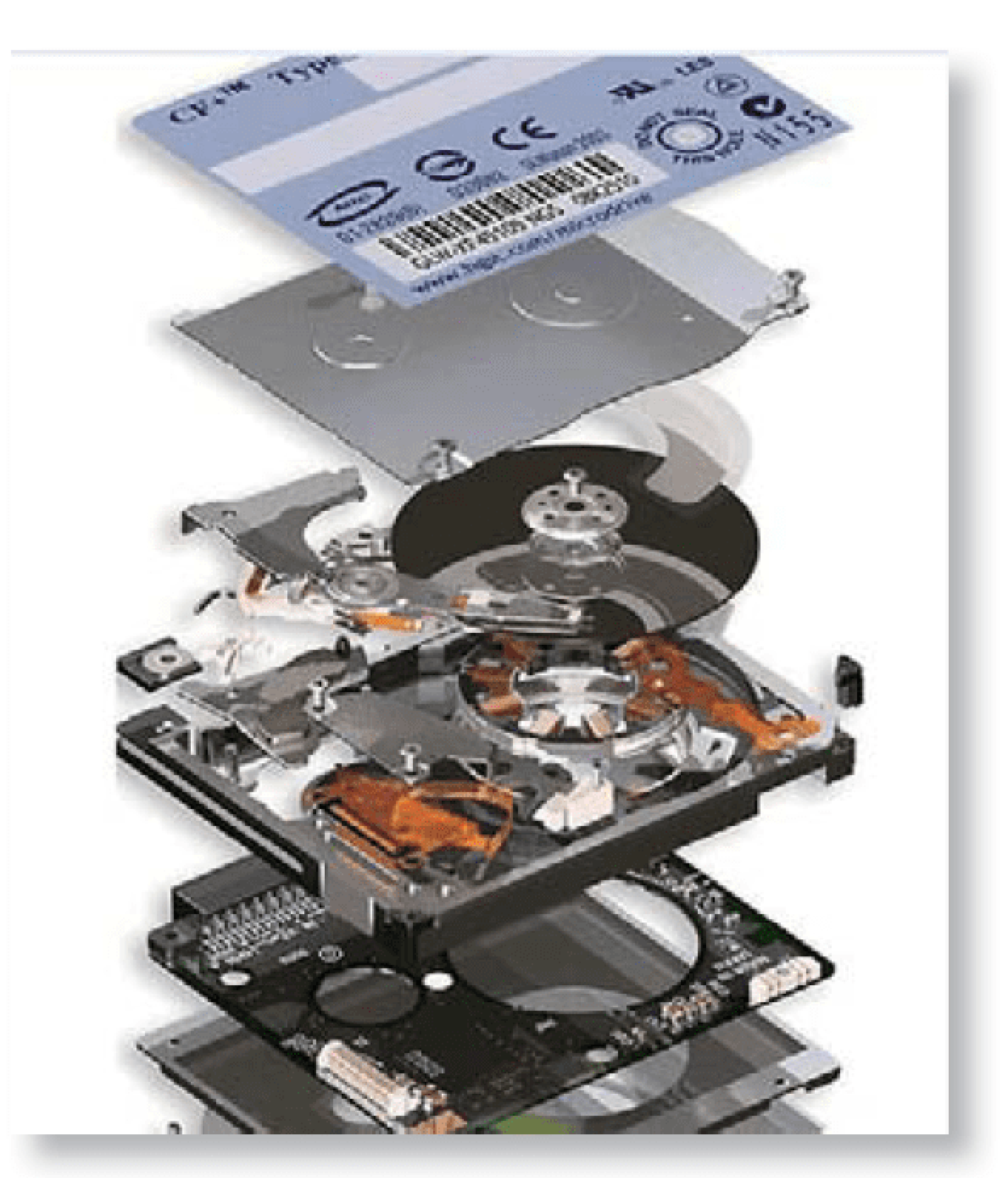
第2招 不同系统中备份文件的访问

如在不同的操作系统中备份了文件，有时会遇到在新的操作系统中不能访问备份文件的情况，这时需对其进行设置，其方法为：打开Windows资源管理器，在其中选择“组织”/“文件夹和搜索选项”命令，在打开对话框的“查看”选项卡中取消选中“使用共享向导”复选框，单击 确定 按钮即可。





第3招 判断硬盘数据损坏的原因



硬盘是非常脆弱的，即使它受到很微小的破坏都可能造成数据的损坏或丢失。因此，要恢复损坏的数据，首先应准确判断硬盘数据损坏的原因，其方法如下：

①加电后，如硬盘没有任何反应，表明硬盘的电路出现了问题；如屏幕显示“磁盘未分配”，则表明硬盘的分区表出现了混乱，致使分区无法识别。

②进入系统后，可以看到数据，但是无法访问或者复制，可能是硬盘出现了坏道；硬盘运转正常，但BIOS检测不到，可能是硬盘初始化信息丢失了。

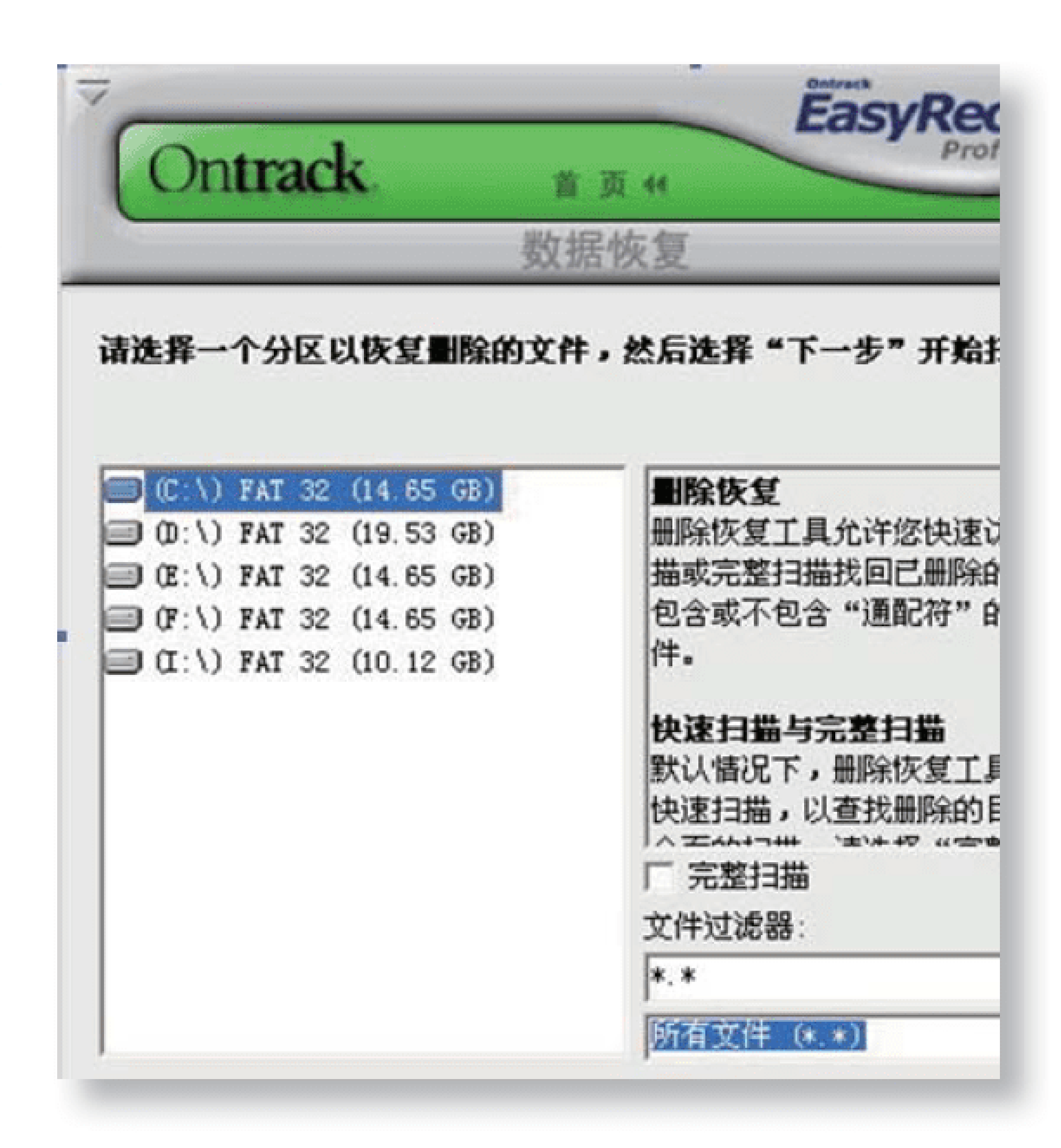
提示：加电后，如听到硬盘发出哒哒的响声或者其他不正常的声音，这时应该马上断电。如果再测试几次，磁头有可能将盘面划伤，资料将彻底被破坏掉。

第4招 使用EasyRecovery简单恢复数据

EasyRecovery是目前最常用到的数据恢复工具，使用其可进行丢失数据的恢复（可恢复误删除的数据、格式化或重新分区后丢失的数据，或因感染病毒、断电和程序的非正常操作等原因造成的数据损坏和丢失），其方法如下：

①启动软件，选择“数据恢复”选项卡，单击右侧窗格中的“删除恢复”超链接，软件会扫描系统，并弹出一个警告窗口，单击 确定 按钮。

②在进入的界面中选择要恢复数据的磁盘，即可开始扫描删除的文件，根据需要进行恢复即可。

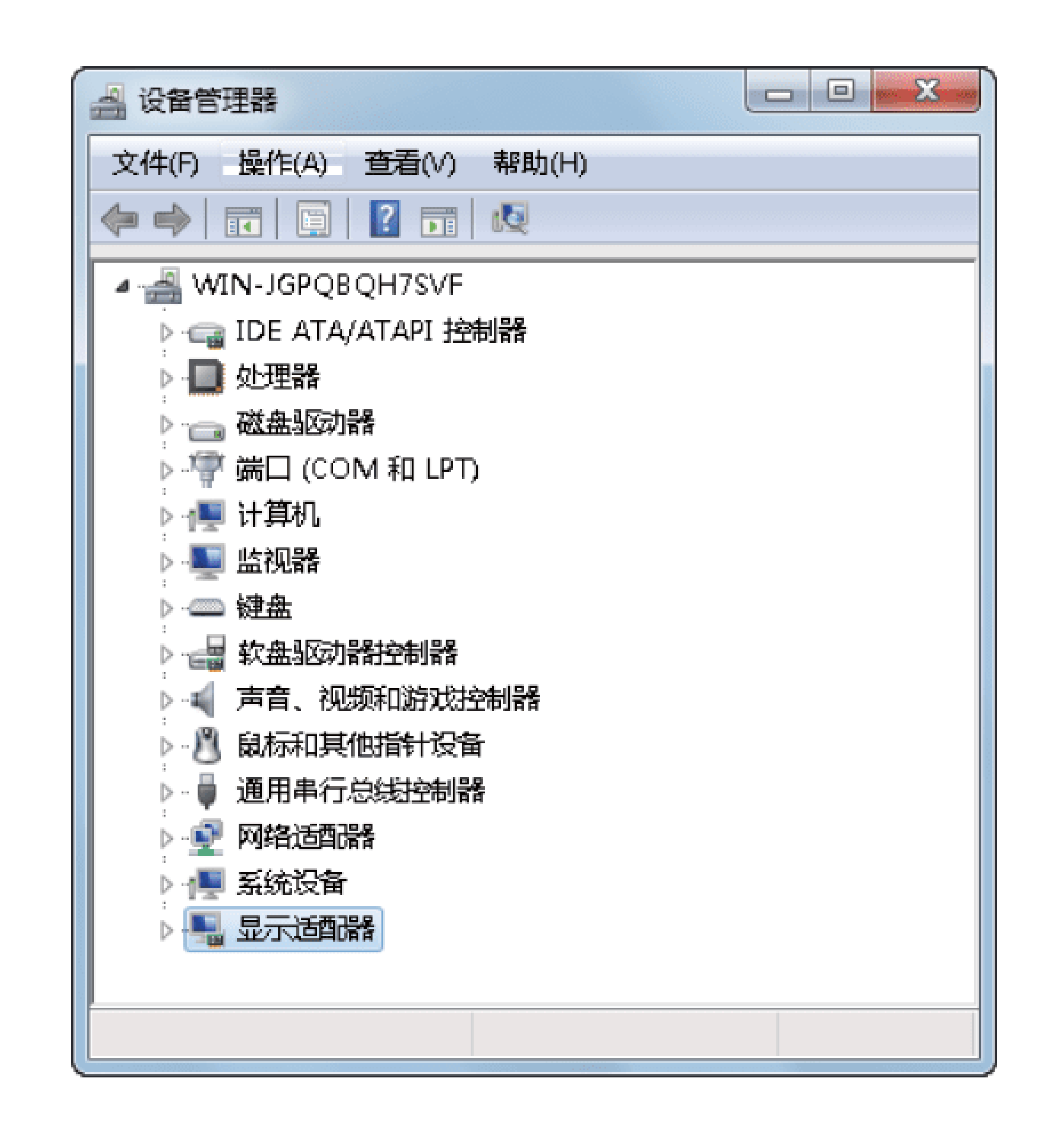


第5招 驱动程序的手动备份

电脑中存放驱动程序的文件夹位于系统盘中Windows目录下的System、System32和Inf 3个文件夹下。用户要备份驱动程序，只需将相应的文件夹进行保存即可，其方法如下：

①在D盘（或除系统盘的任意分区）建立一个临时的“驱动程序”文件夹。

②将C盘Windows目录下的System、System32和Inf 3个文件夹分别复制到D盘的“驱动程序”文件夹中即可。



9.5 活 学 活 用

（1）简述文件在硬盘中的存储原理，并分别对硬盘的组成结构用自己的理解进行概括。

（2）使用FinalData软件进行删除和格式化文件的恢复。

（3）在网上搜索目前流行的文件恢复工具，了解其各自特点，并根据需要选择适合的工具进行使用。

（4）使用相应的软件或工具对注册表及驱动程序进行备份。

（5）利用系统自带的文件备份和恢复功能对系统中重要的文件进行备份。



- ☑ 想知道操作系统的急救有哪些方法吗？
- ☑ 还在为电脑操作系统的崩溃而担惊受怕吗？
- ☑ 想知道怎样使用MaxDOS软件备份和恢复系统吗？
- ☑ 想制作U盘启动和设置从U盘启动吗？



第 10 章 操作系统的急救

娜娜今天很忙，她一大早就来到了公司，打开自己的电脑，但是却发现怎么也进不了操作系统，这可把她给急坏了，没办法，只好等阿伟来了帮她看看到底怎么回事。没多久阿伟便来了，娜娜马上拦着阿伟，让他看看自己电脑出了什么问题，阿伟查看了以后告诉她，只有重新安装操作系统，因为系统文件被损坏了。娜娜这可着急了，她知道安装系统是很麻烦的一件事。阿伟笑着说：“没关系，我那有备份的操作系统，很快就可以给你恢复。”这样娜娜才放下心来，她很好奇，打算跟着阿伟学学怎样恢复操作系统。

10.1 备份和还原操作系统

阿伟为娜娜处理完电脑的问题后，对娜娜说：“现在我需要为你的电脑操作系统进行备份，下次再遇到这种情况可以自己进行恢复。”娜娜点点头，她也想看看阿伟怎样进行备份。阿伟边操作边向娜娜解释道：“要为系统进行备份和恢复等操作通常要用到MaxDOS软件，使用该软件能快速简单地为操作系统进行备份和恢复，将不再担心操作系统的损坏，下面将给你讲解。”

新手解惑

Q：MaxDOS 备份和还原操作系统的原理是什么？

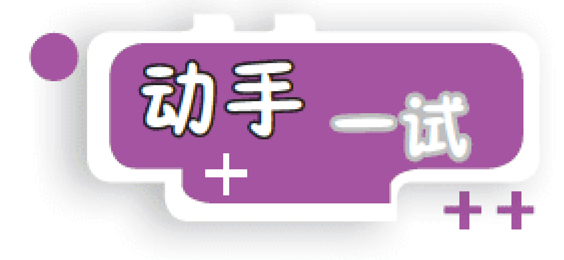
A：在MaxDOS中自带有Ghost软件，Ghost是一款专业的系统备份和还原软件，使用它可以将某个磁盘分区或整个硬盘上的内容完全镜像复制到另外的磁盘分区和硬盘上，或压缩为一个镜像文件。该软件能在启动电脑时方便地进入DOS进行相关操作。

10.1.1 使用MaxDOS软件备份操作系统

在对系统进行备份之前，应该先安装备份软件Ghost，但Ghost只能在DOS下运行，因此可以先安装一个DOS软件——MaxDOS。

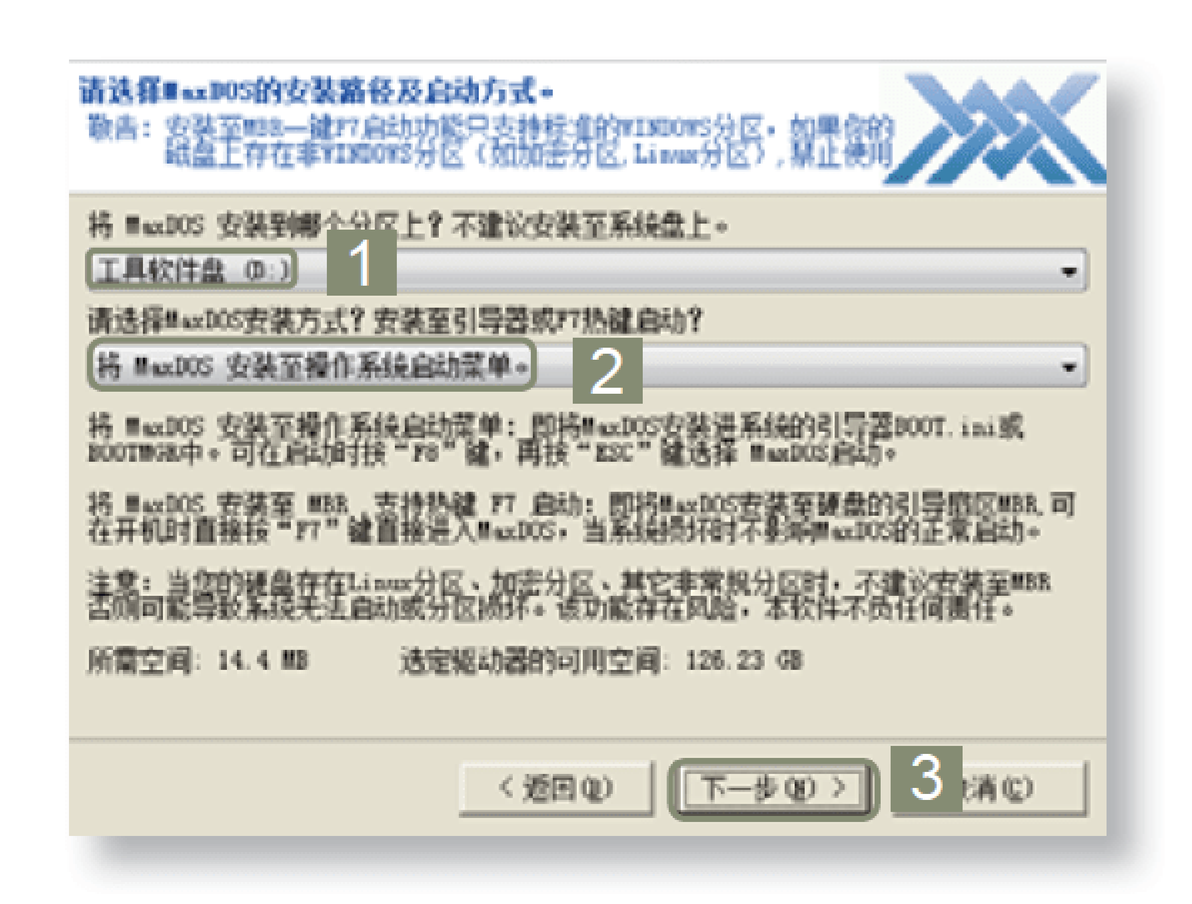
1. 安装并启动MaxDOS

要安装MaxDOS软件，首先需下载该软件的安装程序，再运行安装程序进行安装即可，安装完成后重启电脑，在启动菜单中选择该软件的相应选项，即可将其启动并进入操作界面。



下面将在电脑中安装MaxDOS 9，然后重启电脑进入MaxDOS界面，选择相应选项进入Ghost，其具体操作如下。





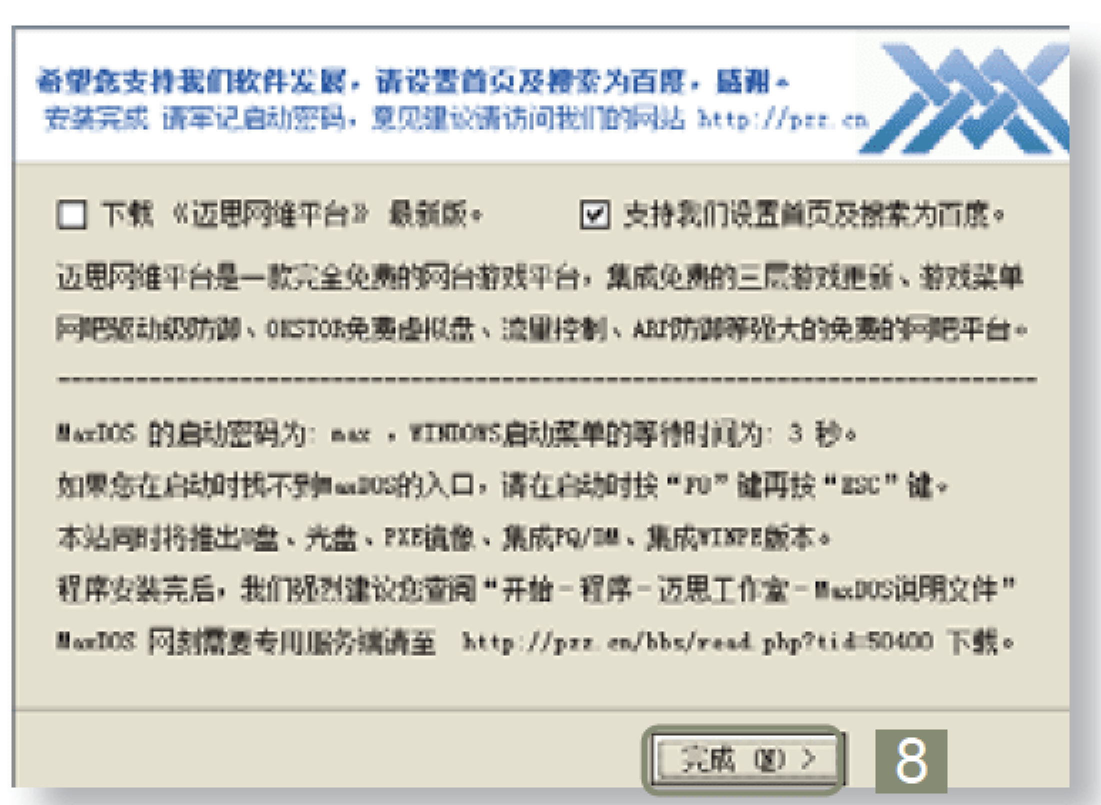
第1步：选择安装盘和启动方式

双击安装程序图标，打开安装向导，在其中单击[下一步(N) >]按钮，然后同意许可协议，在打开对话框的安装位置下拉列表框中选择一个硬盘分区选项，在启动方式下拉列表框中选择“将MaxDOS安装至操作系统启动菜单。”选项，单击[下一步(N) >]按钮。



第2步：设置MaxDOS参数

在打开的对话框中设置MaxDOS，在“请输入Windows启动菜单的等待时间”下拉列表框中输入“3”，在密码下拉列表框中输入“max”，并在备份文件保存位置下拉列表框中选择保存备份文件的位置，然后单击[下一步(N) >]按钮。



第3步：完成安装

系统将开始安装软件并显示安装进度，安装完成后，在打开的对话框中单击[完成(N) >]按钮即可。

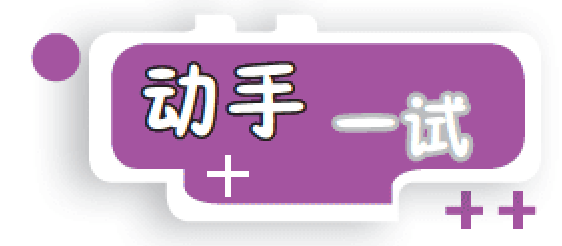


第4步：启动MaxDOS

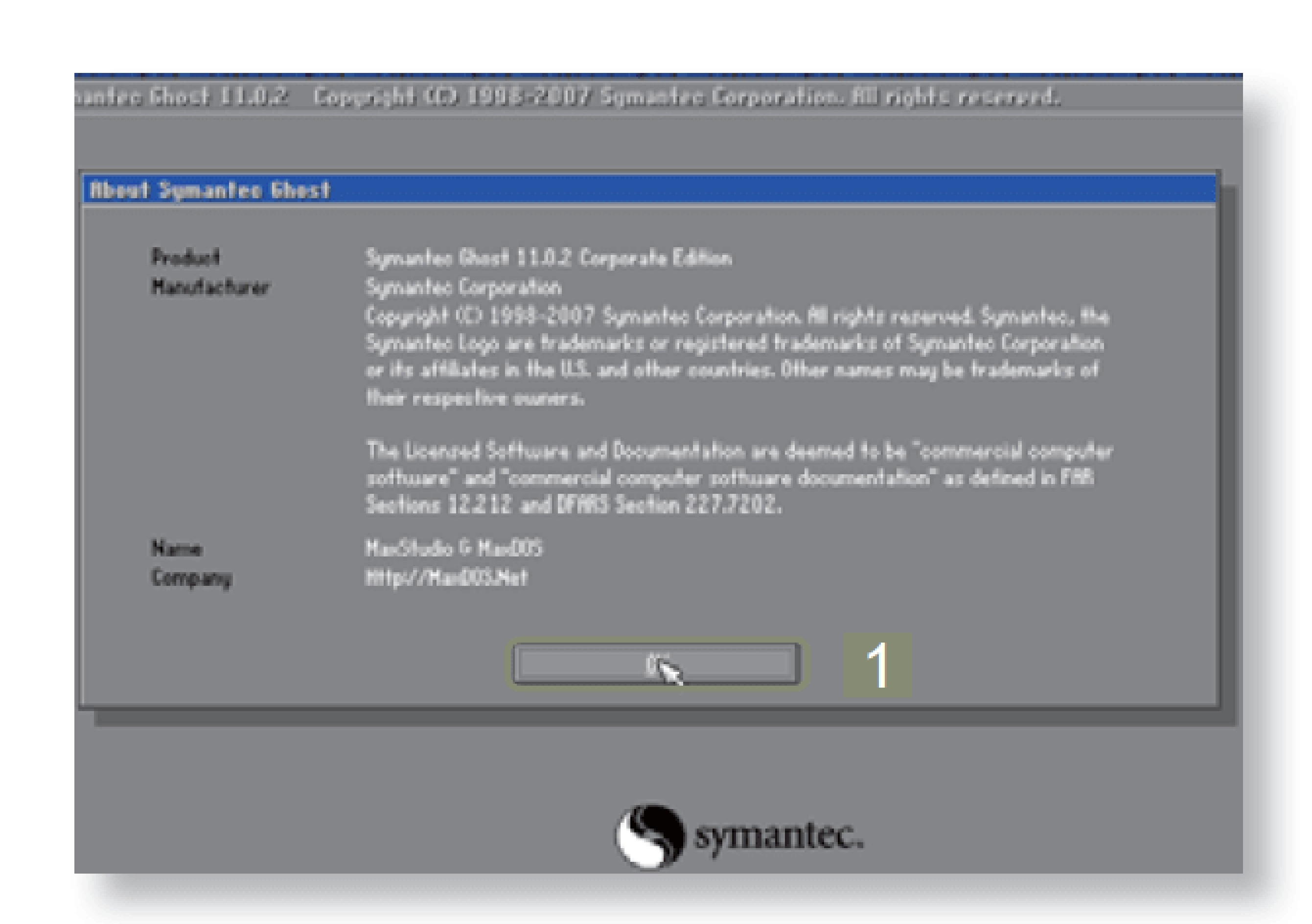
重新启动电脑，在系统进入系统启动菜单时按方向键，选择“MaxDOS 备份、还原、维护系统”选项，进入MaxDOS主界面，然后输入密码“max”进入操作界面，选择“备份/还原系统”选项，在打开的界面中选择“GHOST 手动操作”选项启动Ghost。

2. 备份操作系统

软件安装完成后，即可在其中使用相应功能进行备份，如操作系统安装在C盘，则可对C盘进行备份。



下面将使用MaxDOS 9备份C盘，其具体操作如下。

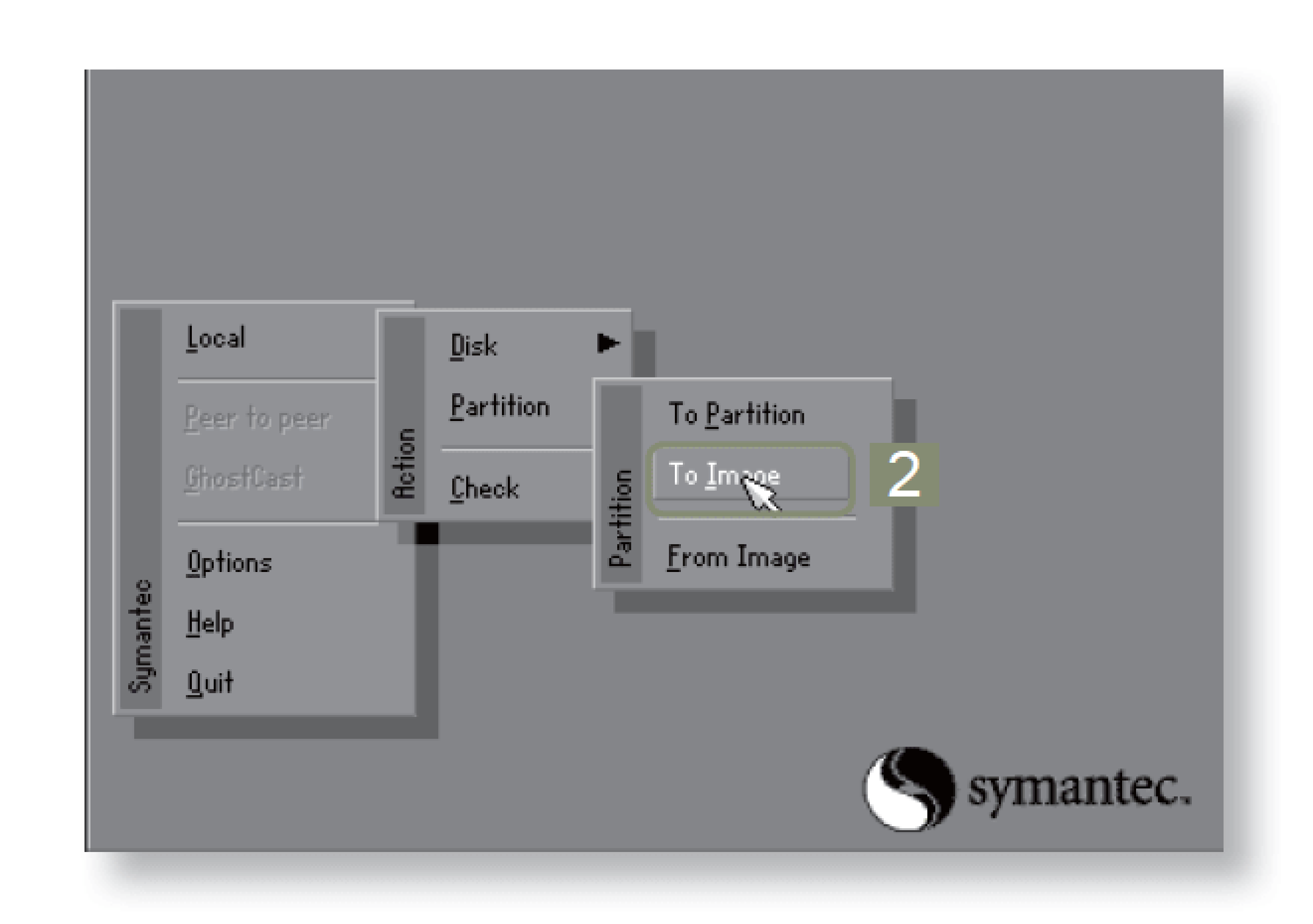


第1步：进入Ghost操作界面

运行MaxDOS软件，根据向导输入密码，然后选择“备份/还原系统”选项，在打开的界面中选择“GHOST手动操作”选项进入Ghost 主界面，在打开的界面中单击 OK 按钮，确认Ghost信息。

第2步：执行备份操作

在打开的Ghost界面中选择Local/Partition/To Image命令，执行备份操作。



提示：选择命令也可通过方向键和Enter键结合使用进行选择。

新手解惑

Q：用Ghost备份与恢复硬盘或磁盘分区都是通过Local菜单中的相应命令实现的，其命令的含义主要包括哪些？

A：Disk：对硬盘进行复制硬盘（To Disk）、将硬盘备份为镜像文件（To Image）和由硬盘镜像文件还原（From Image）等操作。

Partition：对磁盘分区进行操作，它包含的3个命令与Disk菜单下的3个命令相似，不过该菜单下的命令针对的是分区而非整个硬盘。

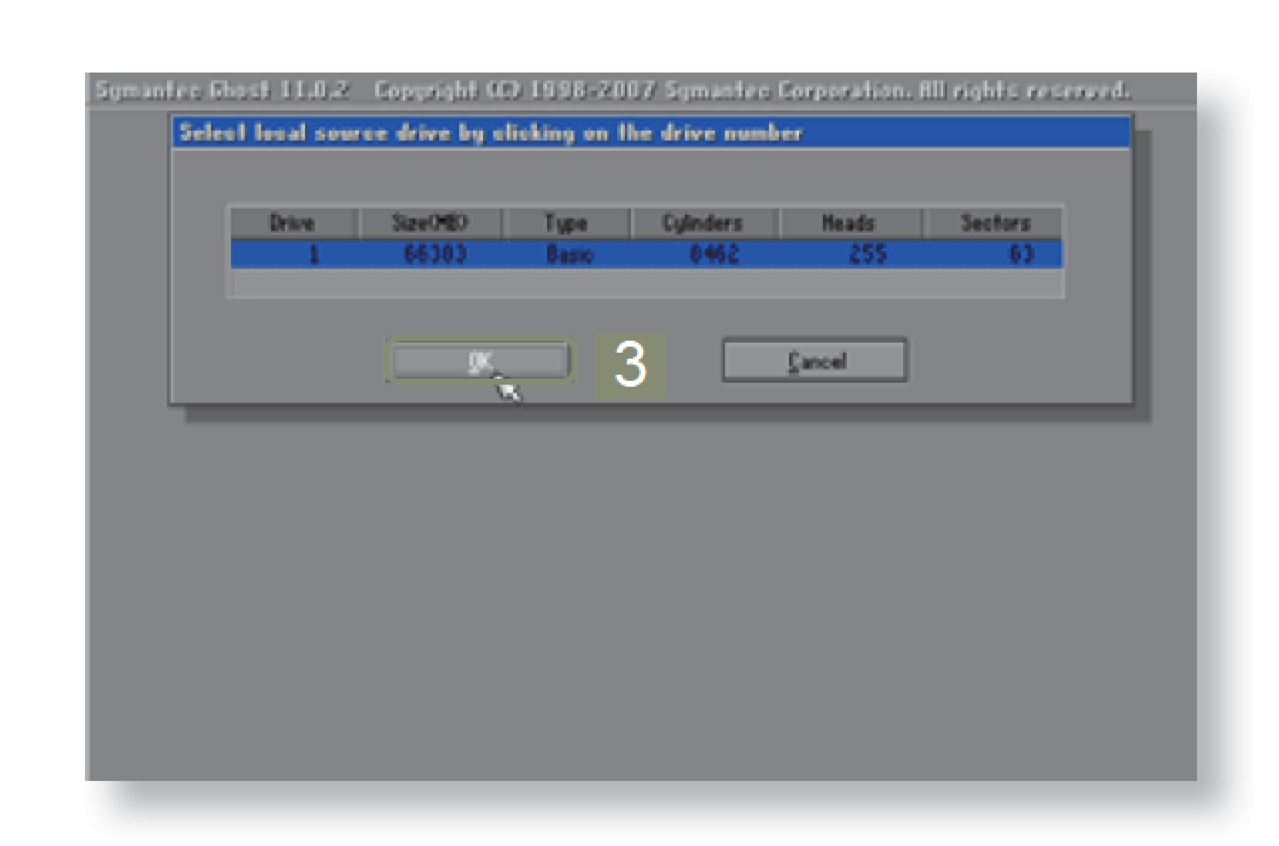
Check：检查磁盘分区是否有坏道或错误。



第3步：选择硬盘

在打开的对话框中选择硬盘，这里直接单击 OK 按钮即可。

提示：如电脑中有多个硬盘，则应选择要备份的操作系统所在的硬盘选项。

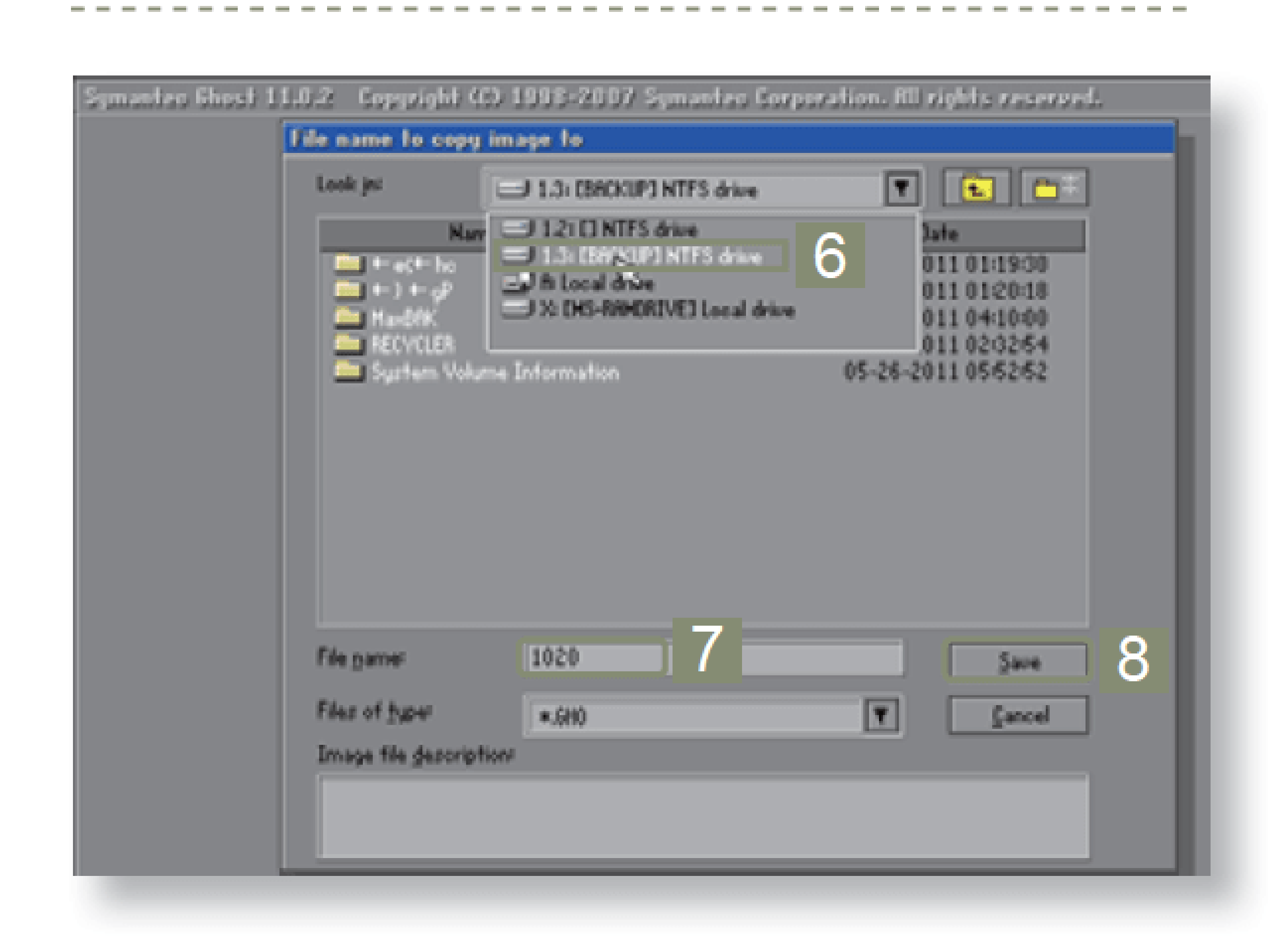


第4步：选择要备份的分区

在打开的对话框中选择要备份的分区，这里选择系统盘所在的第一分区，然后单击 OK 按钮，确认并打开File name to copy image to对话框。

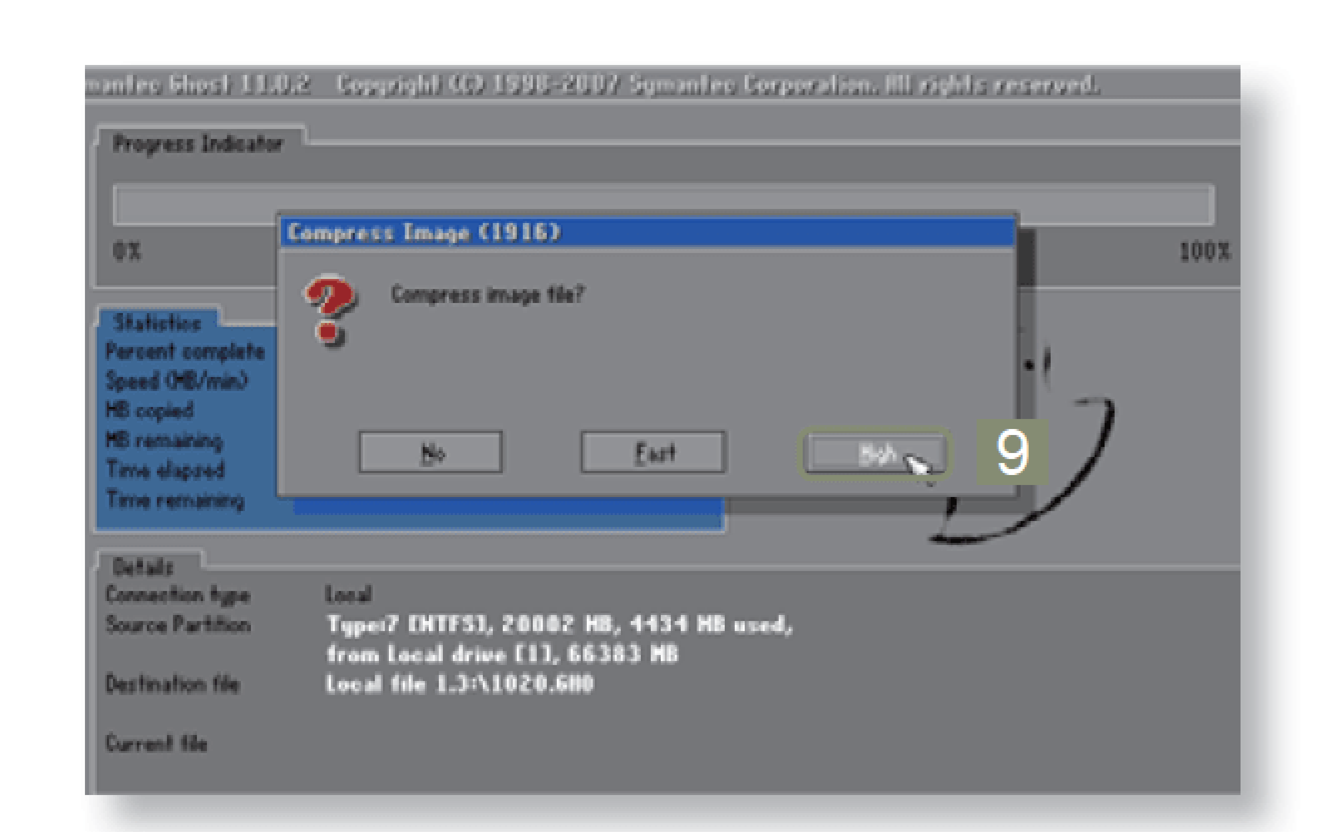
第5步：设置保存位置

在打开对话框的Lock in下拉列表框中选择要保存的位置，这里选择第二个分区，在File name文本框中输入名称，这里输入“1020”，然后单击 Save 按钮确认设置。



第6步：选择文件压缩方式

在打开的对话框中选择文件的压缩方式，这里单击 High 按钮，选择高压缩方式，然后在打开的对话框中单击 Yes 按钮确认创建镜像文件。



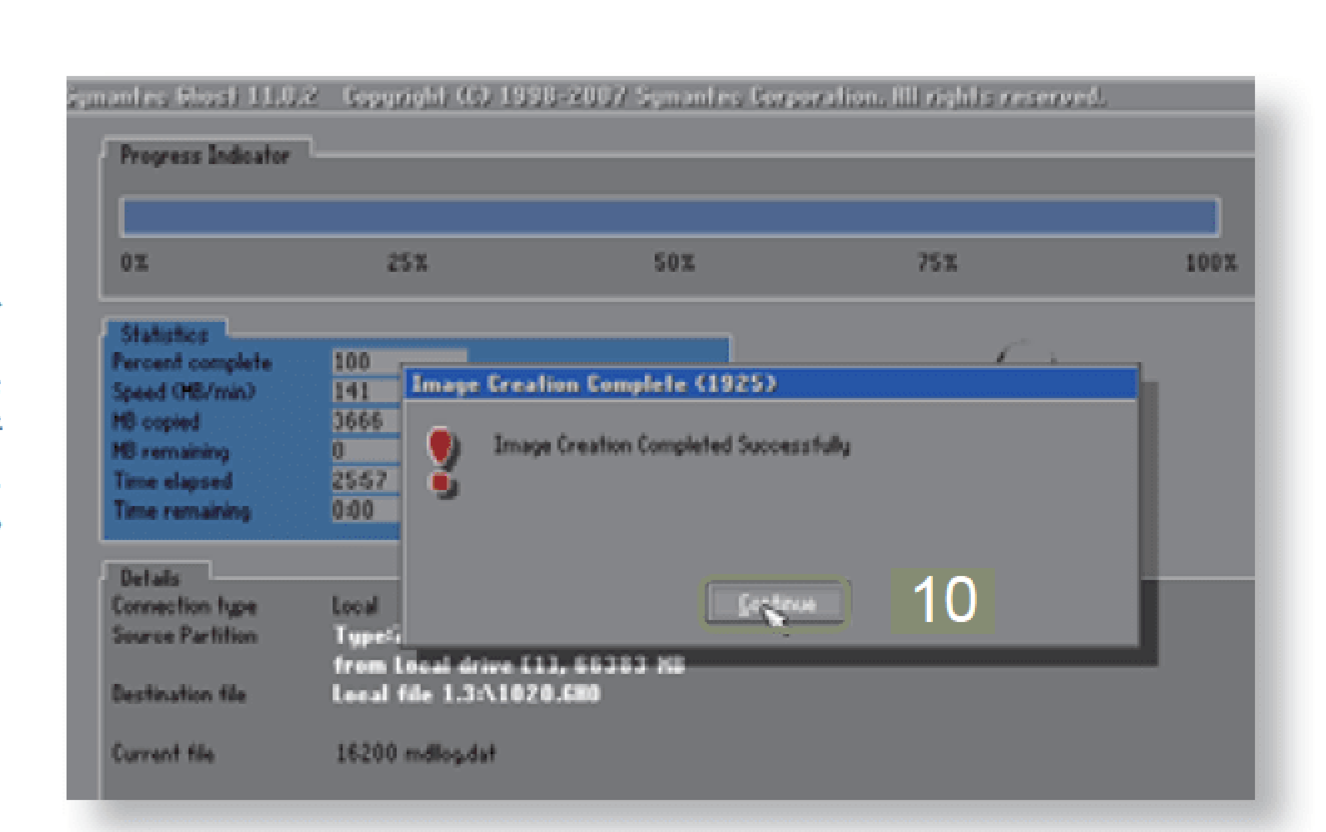


怎样选择文件的压缩方式？

如果要节省磁盘空间，则应选择高压缩方式，如果剩余的磁盘空间相当大，要想追求备份速度，则选择不压缩或快速压缩方式。备份的速度与电脑硬件的配置高低、备份磁盘内容的多少有关，如果电脑配置较好，备份Windows系统的速度相当快。

第7步：完成备份

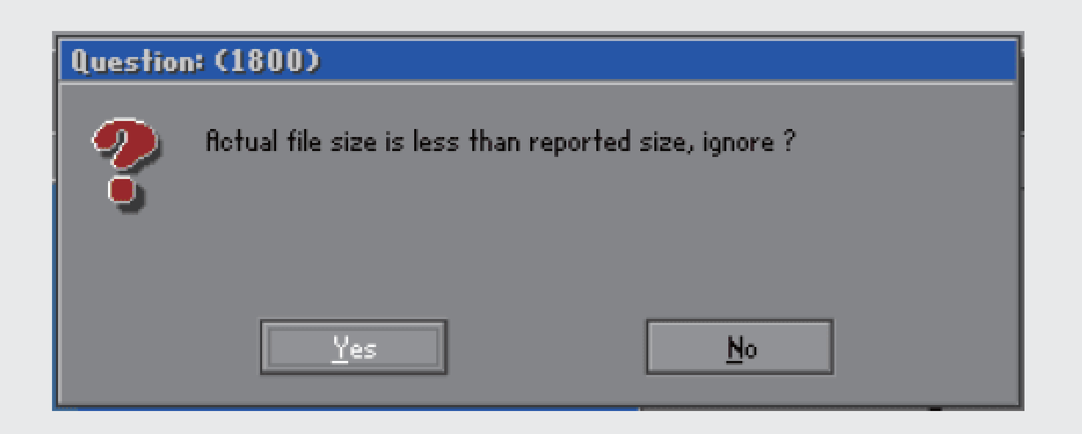
软件开始备份第一分区，并显示备份进度，备份完成后将打开提示对话框提示备份成功，单击Continue按钮完成备份。



教你一招

备份过程中遇到的问题

在Ghost进行备份的过程中，如自动打开对话框，提示用户要备份的分区上的文件总量小于Ghost软件最初报告的总量（一般由虚拟内存文件造成），是否继续进行备份操作。单击Yes按钮即可继续进行备份操作。



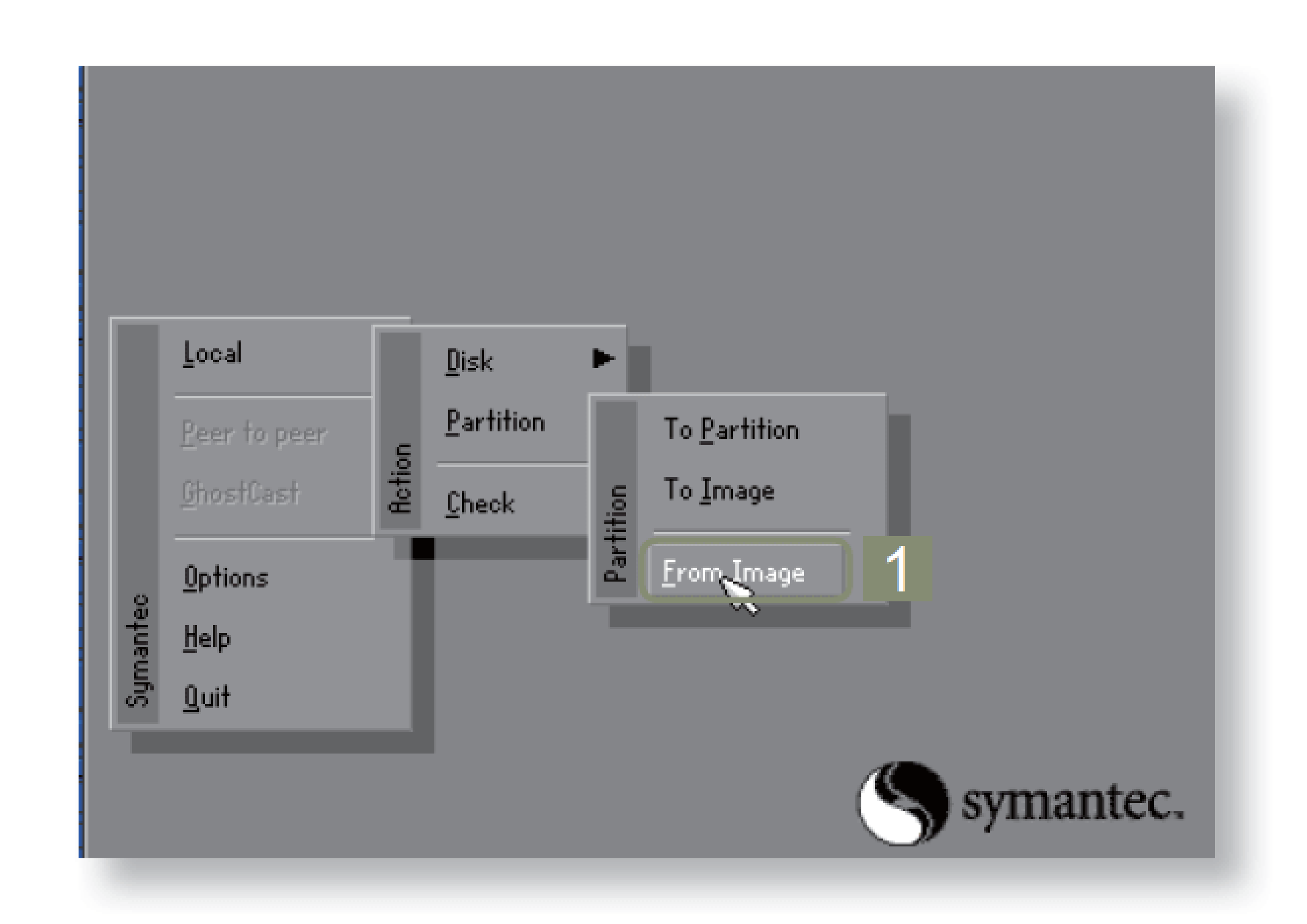
10.1.2　使用MaxDOS还原操作系统

当系统感染了恶性病毒或遭到严重损坏时，可使用MaxDOS将备份的镜像文件快速还原，在进行还原时，如备份的是C盘，则只能还原到C盘，否则将出现错误。





下面将使用MaxDOS 9还原备份的操作系统，其具体操作如下。

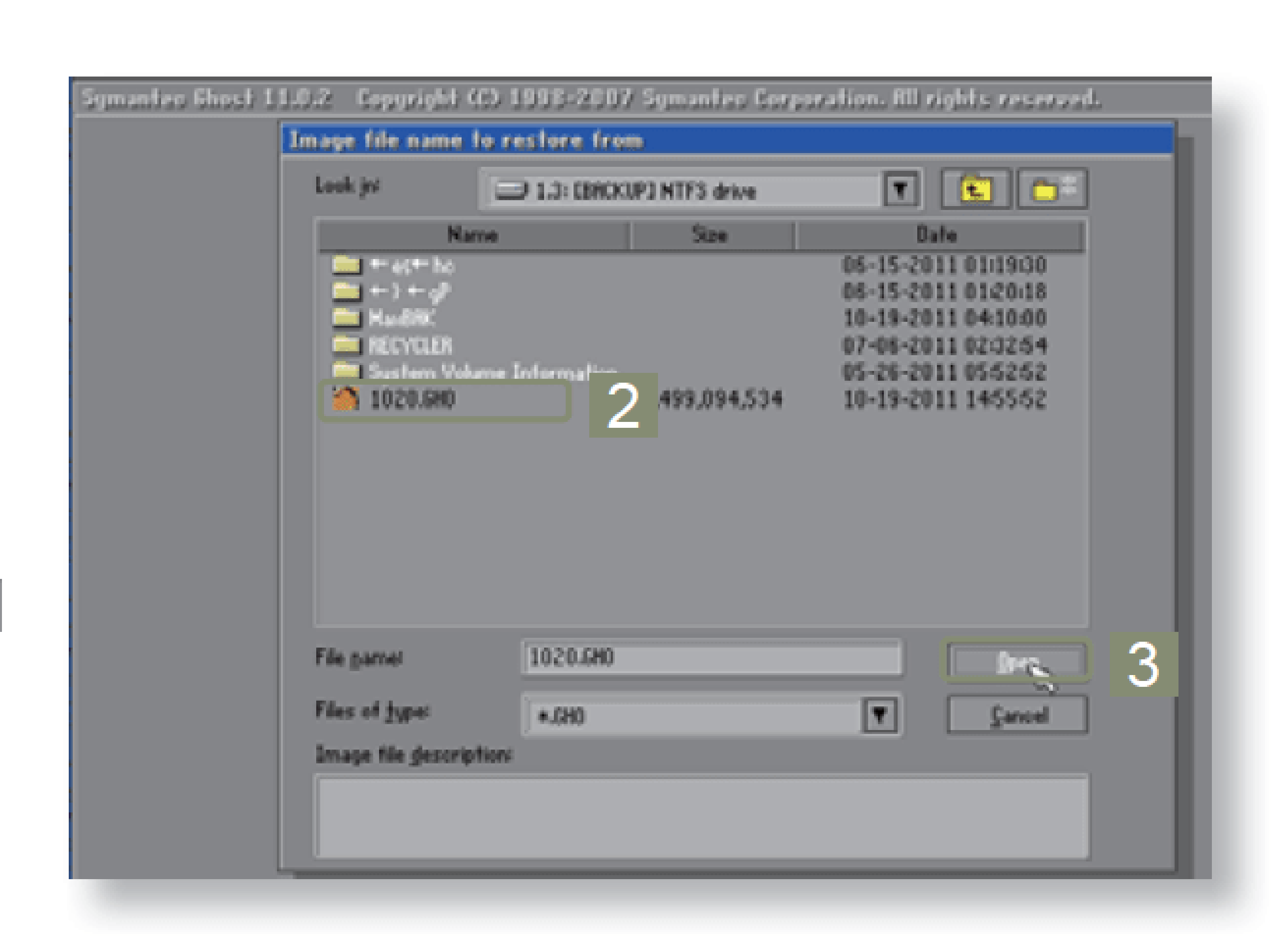


第1步：执行还原操作

打开Ghost界面，在其中选择Local/Partition/From Image命令，执行还原操作，并打开Image file name to restore from对话框。

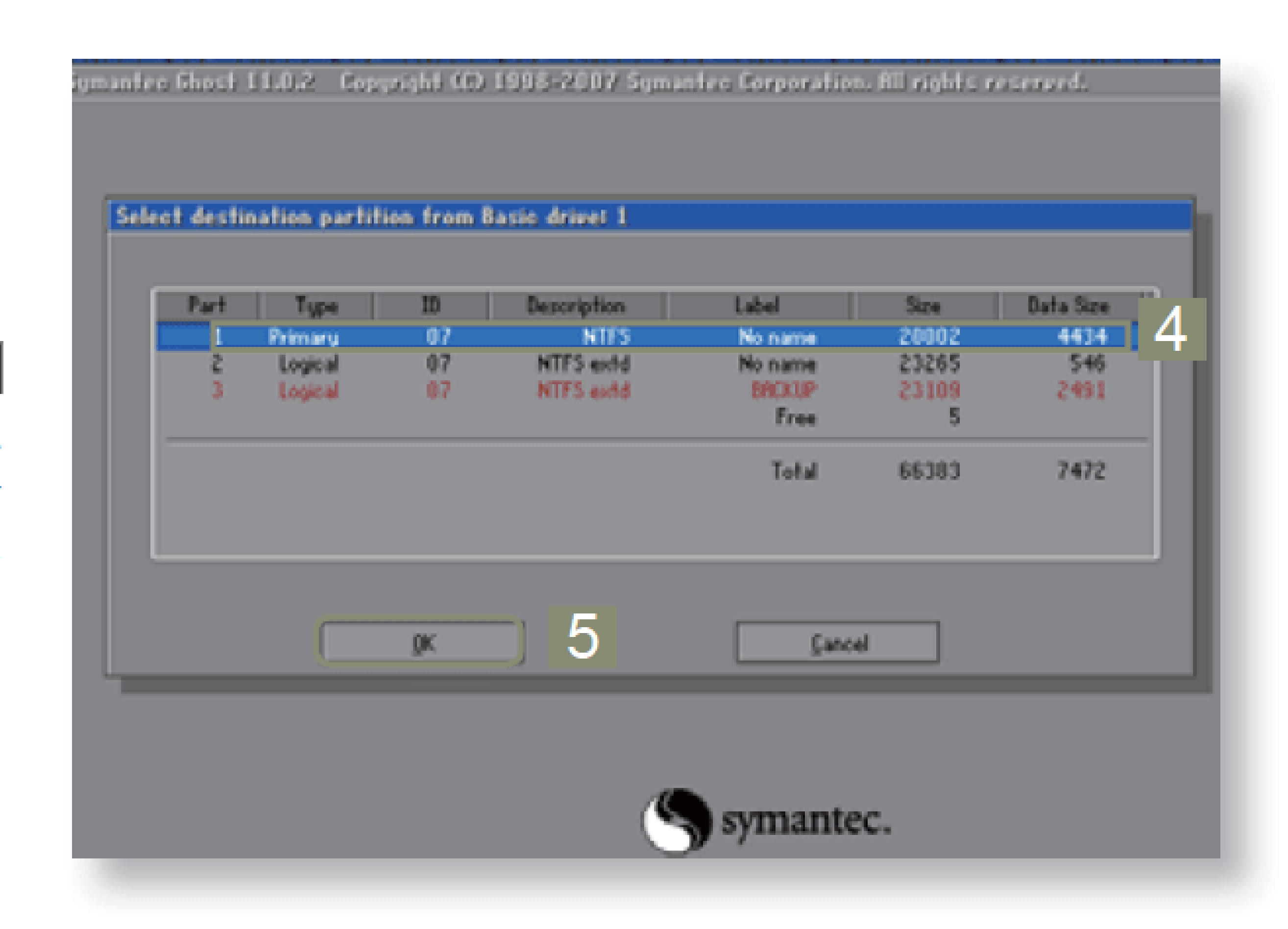
第2步：选择要还原的镜像文件

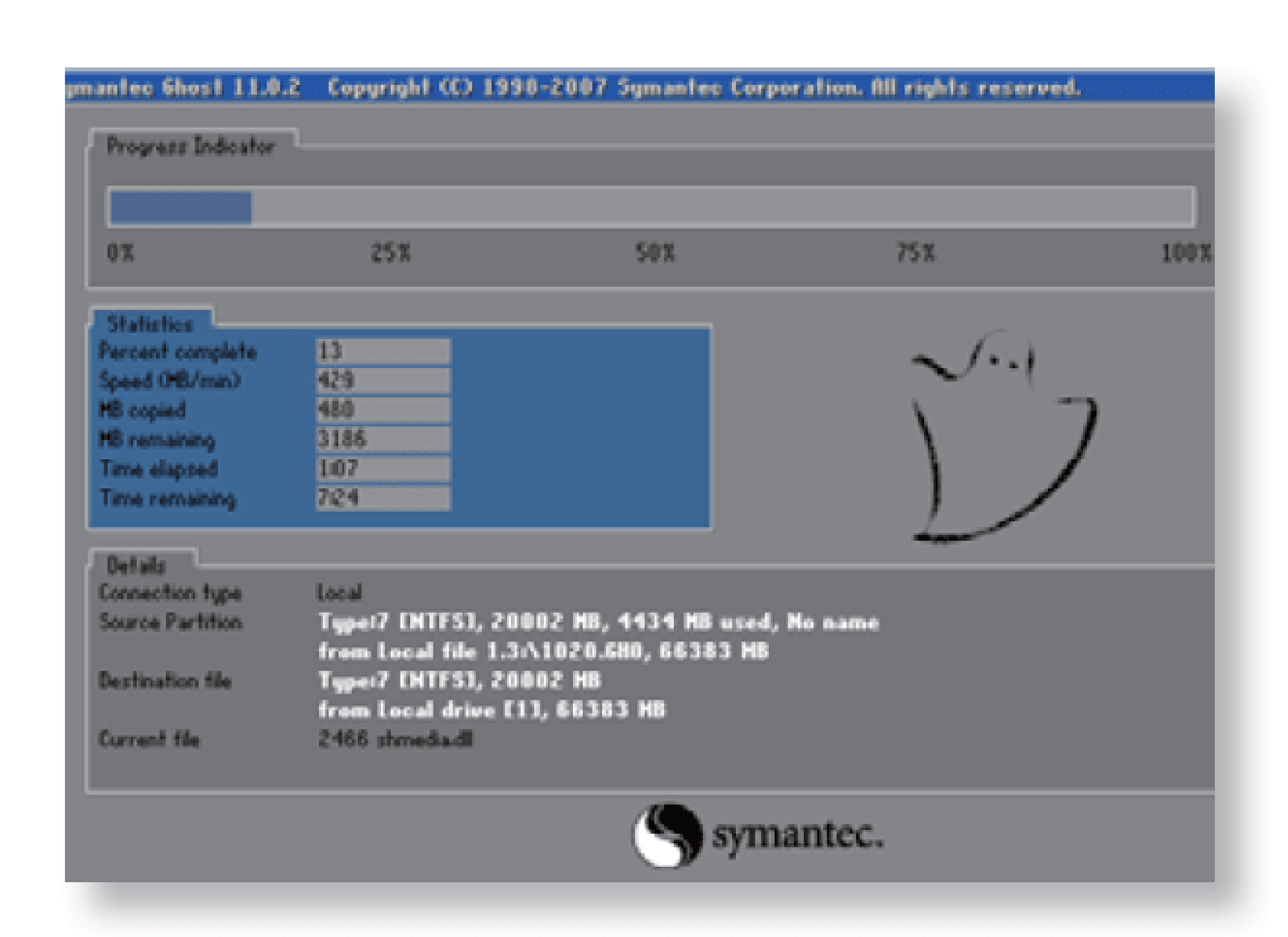
在打开的对话框中选择前面备份的镜像文件，然后单击Open按钮，在打开的对话框中显示了该镜像文件的大小及类型等相关信息，单击OK按钮确认信息。



第3步：选择要还原的分区

在打开的对话框中选择需要恢复到的硬盘，这里保持默认，单击OK按钮，在打开的对话框中选择需要恢复到的磁盘分区，这里选择第一分区，单击OK按钮。



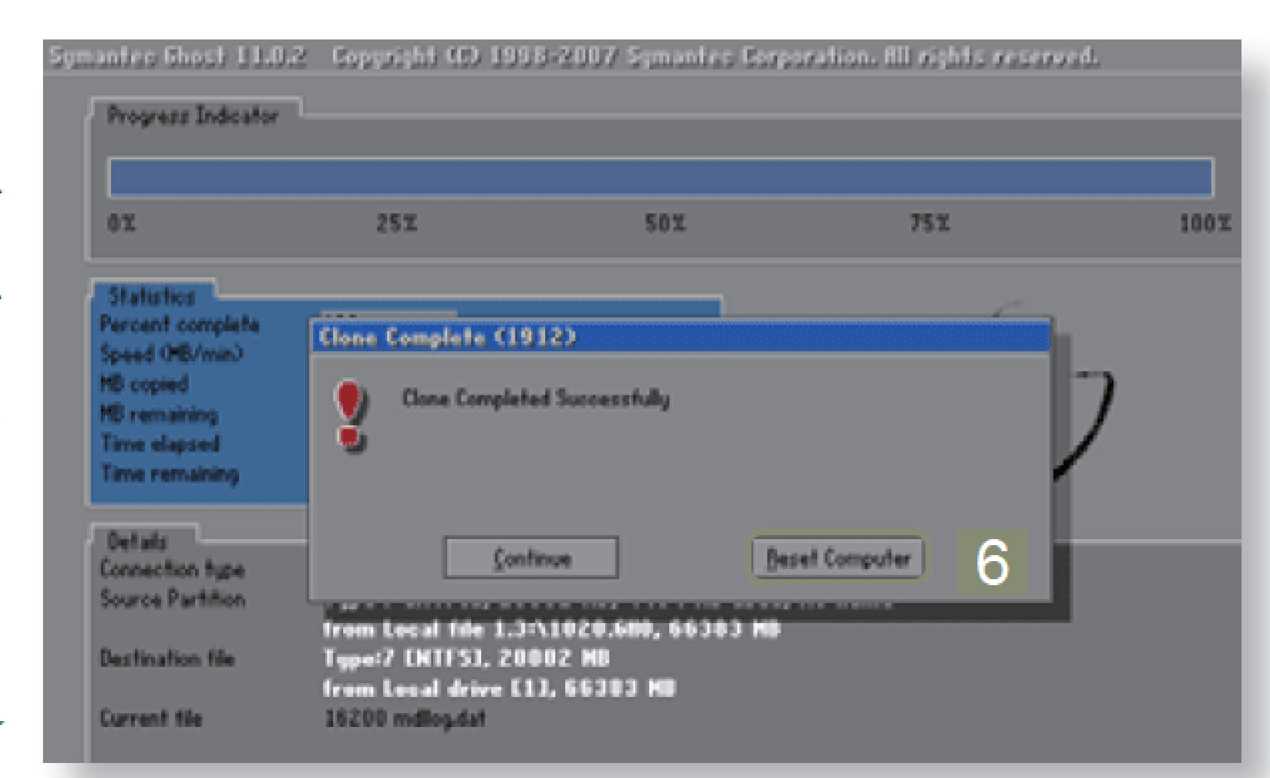


第4步：开始还原

在打开的对话框中单击 Yes 按钮，确认恢复，然后软件开始恢复该镜像文件到系统盘，并显示恢复速度、恢复进度和剩余时间等信息。

第5步：完成还原

恢复完成后，系统将打开提示对话框询问用户是否重启电脑，单击 Reset Computer 按钮即可重启电脑，完成系统的还原操作。

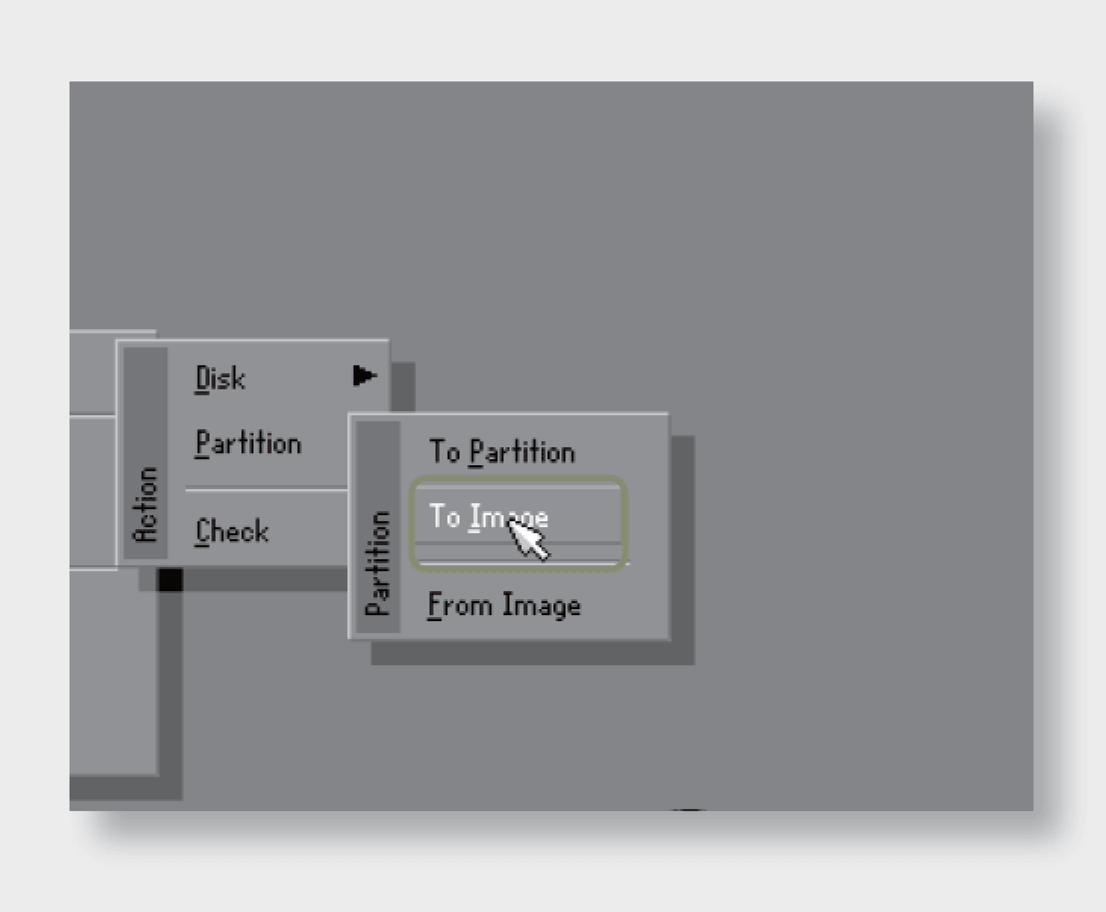


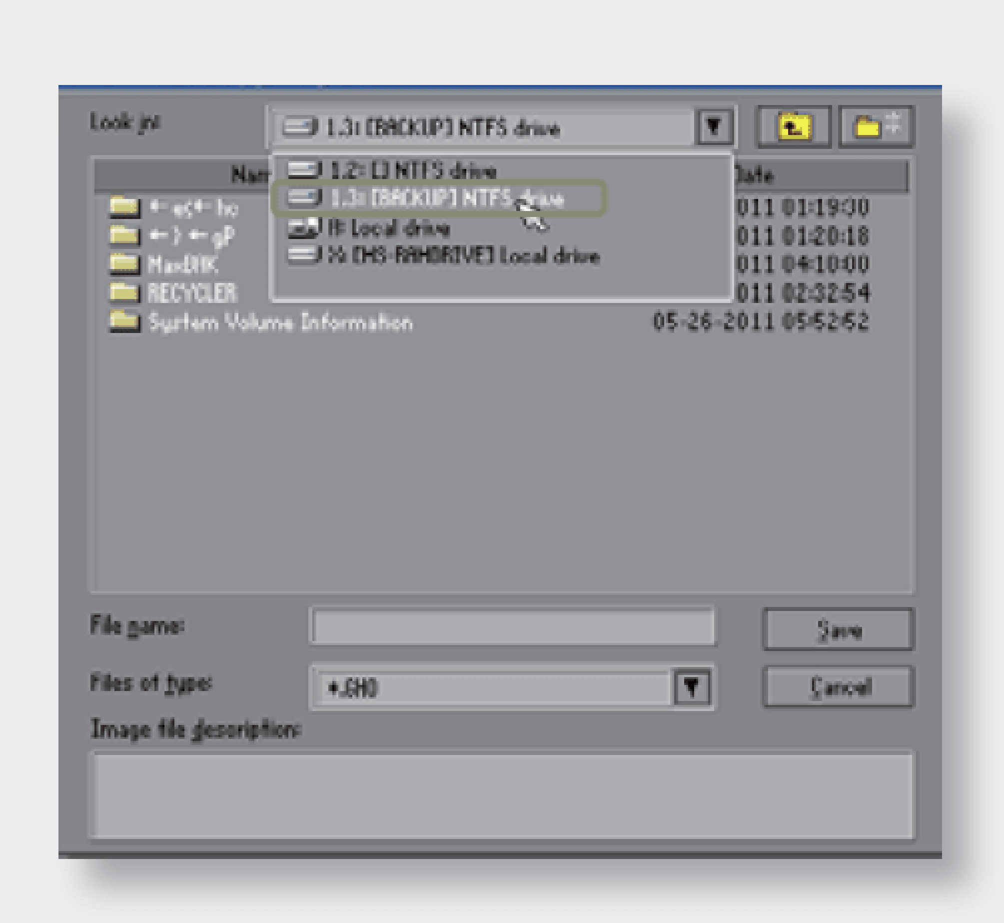
提示：如单击 Continue 按钮，将返回Ghost界面继续进行相关操作。

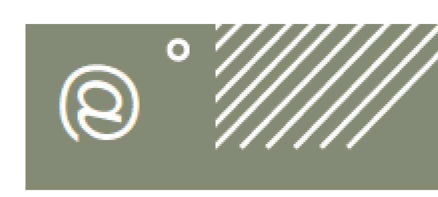
跟我练习

娜娜在听了阿伟的讲解后，想再练习一下备份操作系统的操作

重启电脑，运行MaxDOS软件，进入Ghost界面，选择Local/Partition/To Image命令，在打开的对话框中选择要备份的操作系统分区，根据向导进行操作，直到完成备份操作。







10.2 重装操作系统

阿伟告诉娜娜："如果想要一个'干净'的操作系统，可以将系统进行重装。这样便可以减少占用的电脑资源。"娜娜听了以后问阿伟："如果没有安装光盘可以进行系统的重新安装吗？我这里没有系统盘呢。""那没关系，我可以教你做一个U盘启动来进行安装。"接下来阿伟就向娜娜讲起了重装系统的知识和方法。

10.2.1 重装系统前的准备

如果硬盘中没有操作系统的备份，要重装系统时需要启动到DOS状态下使用安装光盘进行，因此，制作一个DOS启动盘就变得非常必要，同时还要在BIOS中设置U盘启动，并对硬盘分区的容量调整到适合后才能进行系统的重装。

1. 制作U盘启动

要制作U盘DOS启动盘，需使用购买U盘时商家提供的驱动程序安装光盘或U盘启动的相关制作工具来进行。



下面将以使用USBoot工具制作U盘启动为例进行讲解，其具体操作如下。

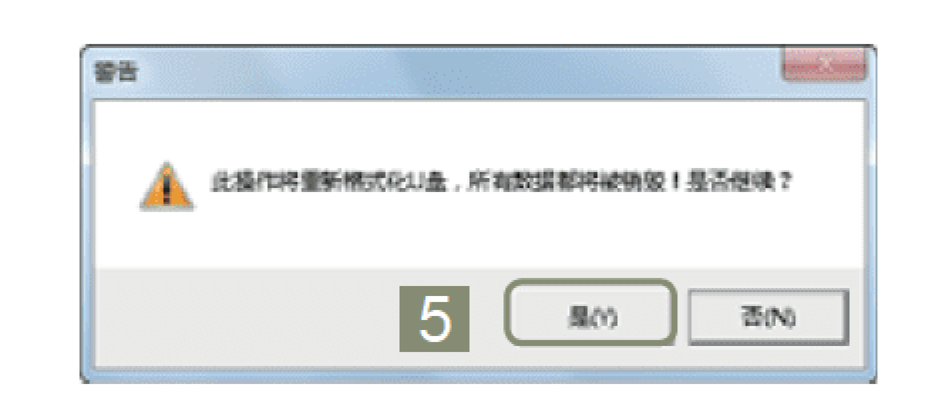
第1步：选择要制作启动的U盘

将U盘插入USB接口，然后启动USBoot程序，在其列表框中选择要制作U盘启动的U盘选项，然后单击"点击此处选择工作模式"超链接，在弹出的菜单中选择"HDD模式"命令，然后单击 开始 按钮即可。



第2步：确认操作

在打开的提示对话框中单击[是(Y)]按钮确认操作的正常进行。



提示：如U盘中存在重要数据，应将其进行备份后再操作。



第3步：制作U盘启动

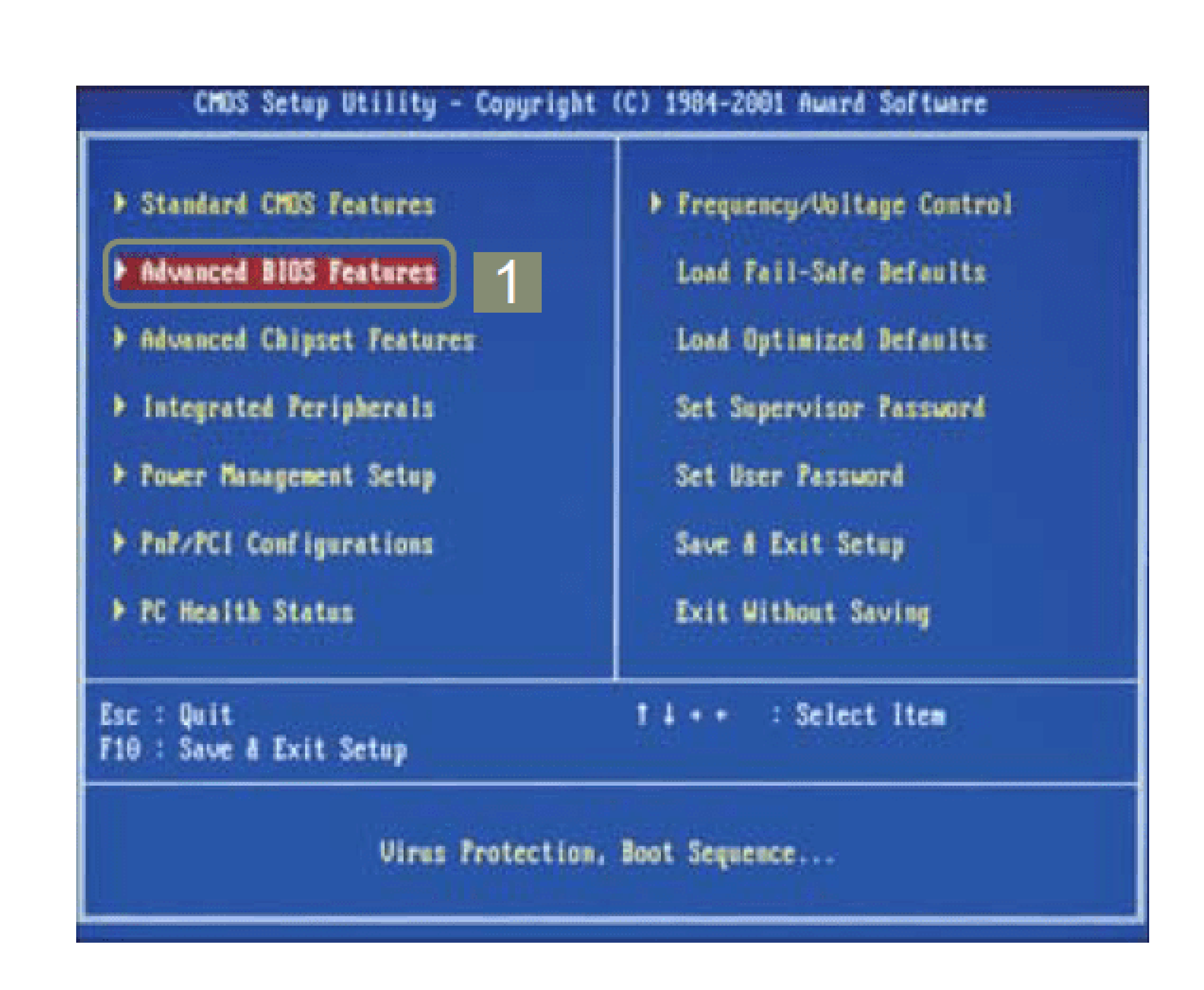
软件将开始对U盘进行处理，在此过程中会提示用户拔插一次U盘，制作完成后，将提示U盘启动制作完毕，完成后单击[×]按钮关闭程序即可。

2. 设置电脑从U盘启动

制作好U盘启动盘后，当需要使用其将系统引导到DOS状态下时，必须先在BIOS中将启动顺序设置为从U盘启动。



下面将在BIOS界面中设置从U盘启动，其具体操作如下。



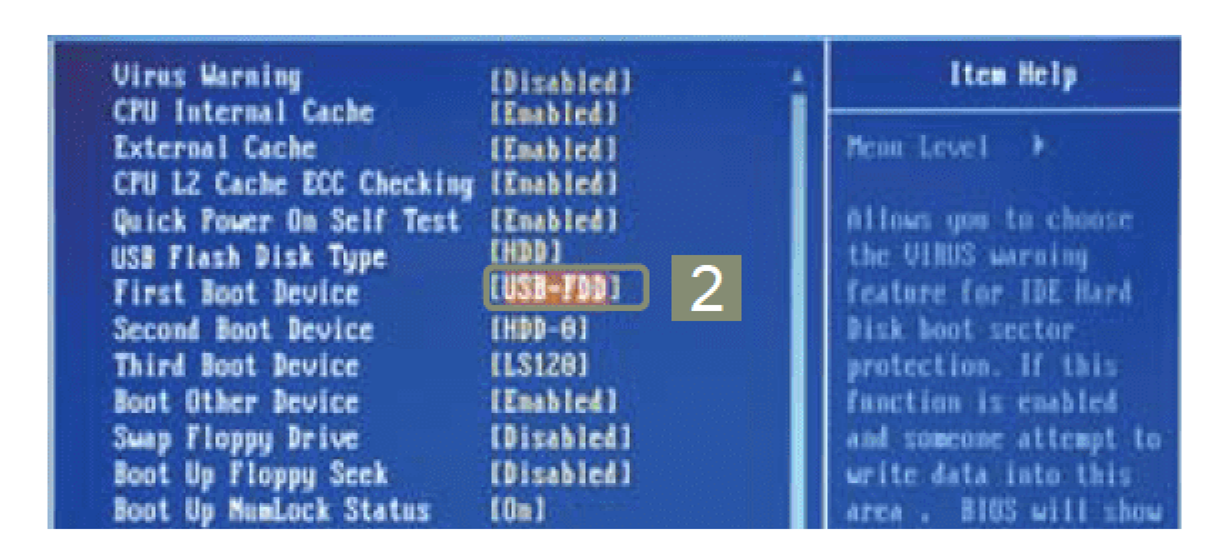
第1步：选择BIOS选项

启动电脑后一直按Delete键，直到进入BIOS界面，通过方向键选择“Advanced BIOS Features（高级BIOS特性）”选项，然后按Enter键进入。



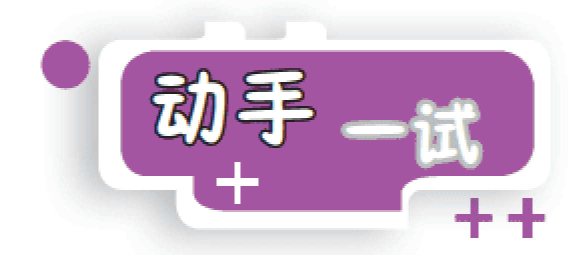
第2步：设置从U盘启动

在打开的界面中将First Boot Device选项设置为USB-FDD，返回BIOS主界面，然后按F10键保存BIOS设置。

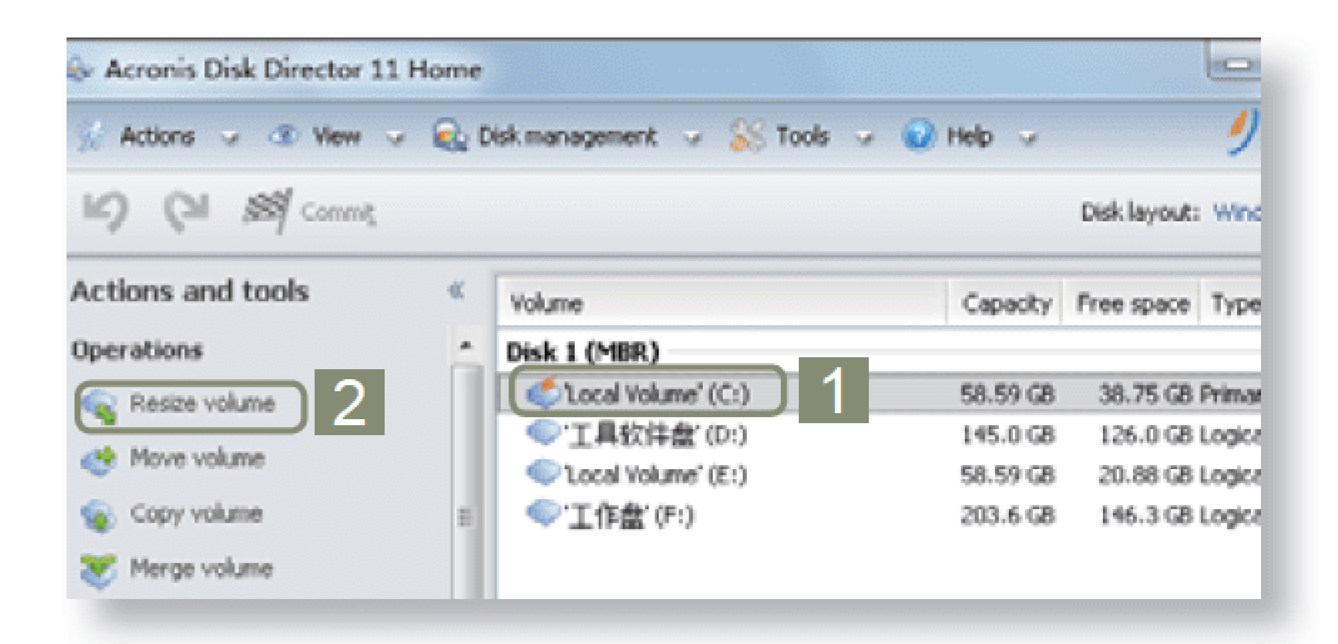


3. 使用Acronis Disk Director 11 Home调整分区容量

用户在重装系统前如发现原来的分区方案不合理，但由于其中存储有数据，因此不能使用Fdisk对硬盘调整分区大小时，可以使用无损分区软件——Acronis Disk Director 11 Home（下载地址为http://www.skycn.com/soft/18511.html）来调整。



下面将使用Acronis Disk Director 11 Home调整C盘容量，其具体操作如下。

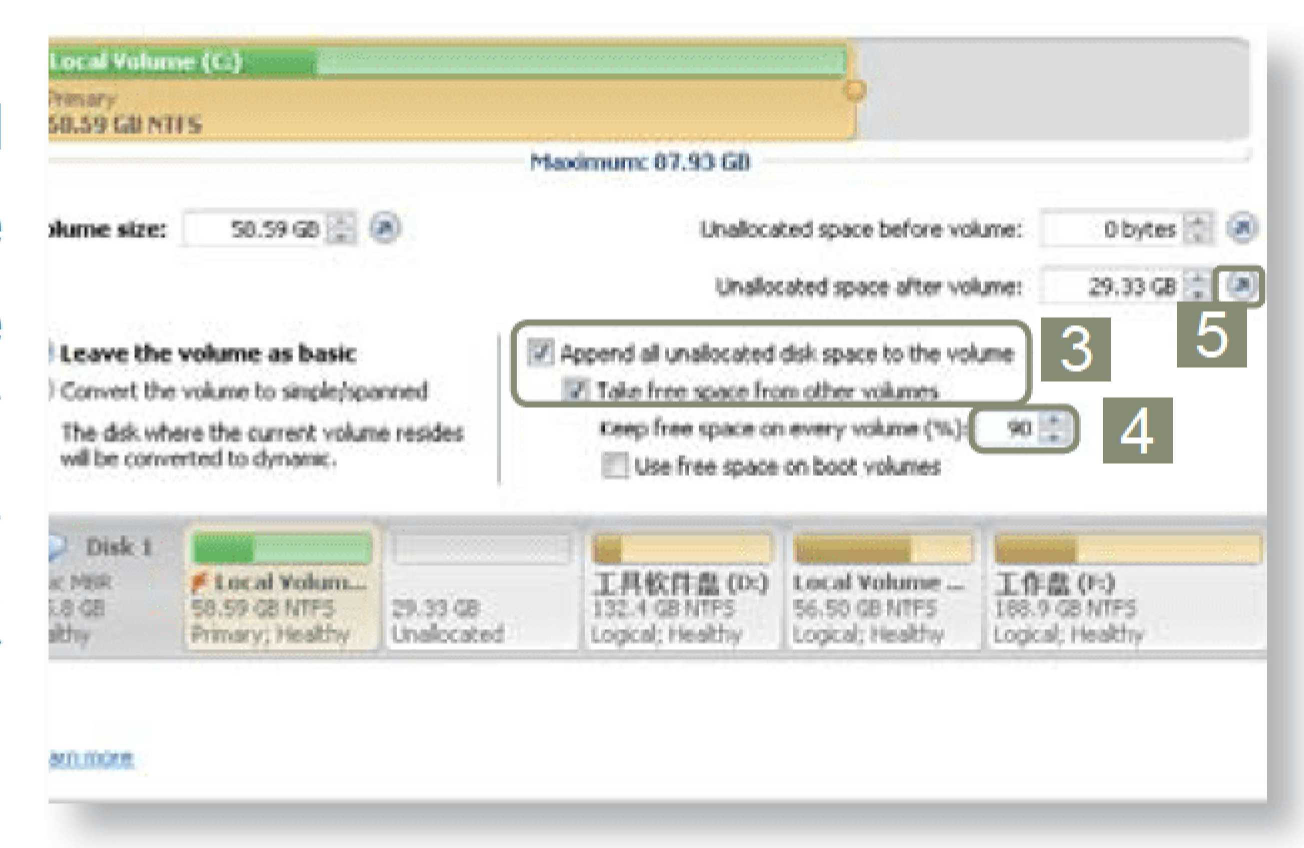


第1步：打开分区大小调整向导

电脑中安装Acronis Disk Director 11 Home软件后，双击其快捷方式，在打开界面右侧的列表框中选择C盘，然后在左侧的功能选项中选择Resize volume选项。

第2步：设置要划分空间的大小

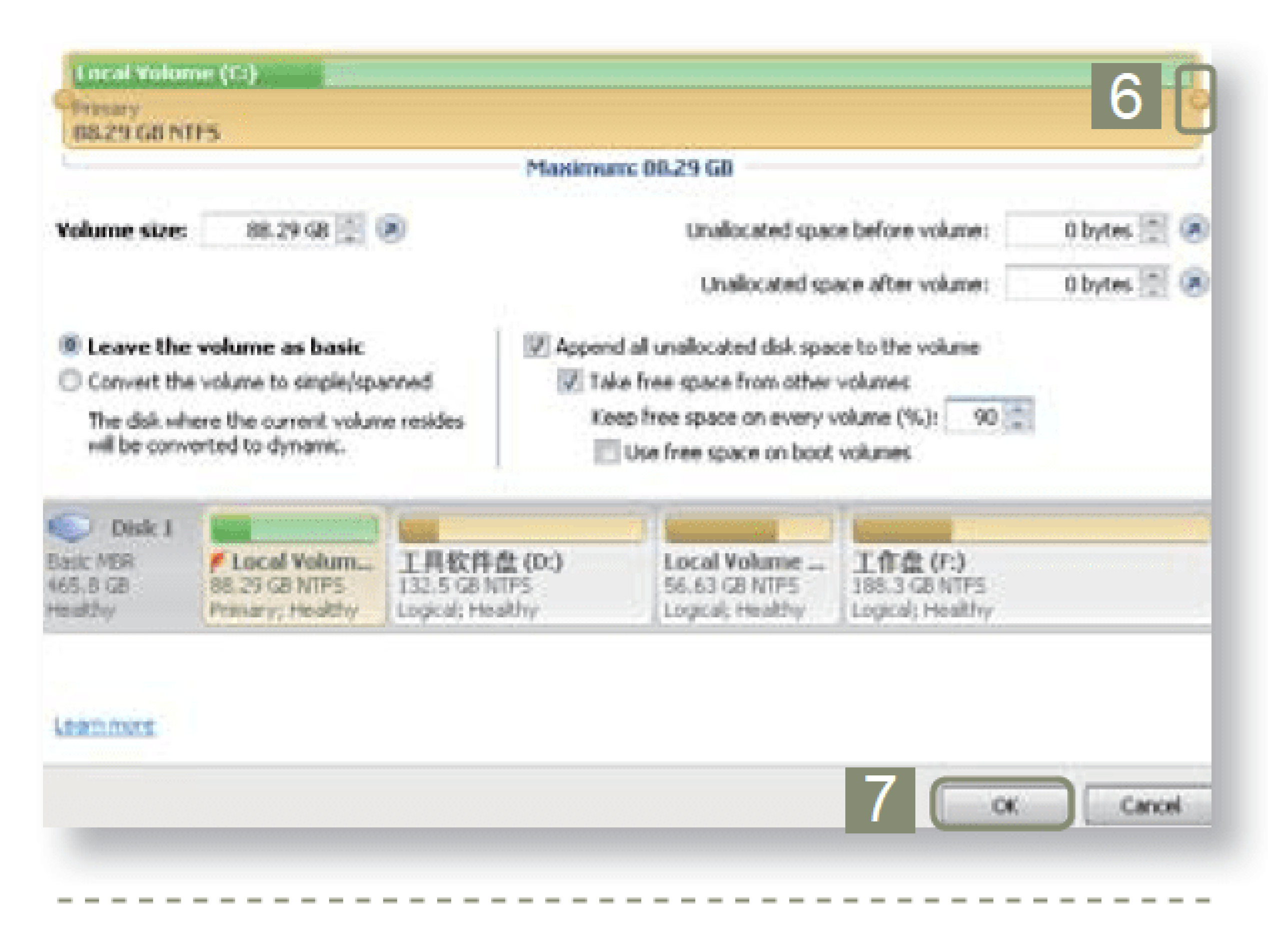
在打开的对话框中选中Append all unallocated disk space to the volume和Take free space frome other volumes复选框，在其下面的数值框中输入“90”，然后单击Unallocated space after volume数值框右侧的按钮，数值框中将显示划分空间大小。



教你一招

划分磁盘空间的方法

Keep free space on every volume数值框表示其他盘中剩余空间保留的百分数，数值越大，保留空间越多，划分到C盘的空间越小。



第3步：调整C盘空间

将光标移动到窗口上方的图标上，然后拖动鼠标，直到Unallocated space after volume数值框显示为0bytes，最后单击OK按钮即可。

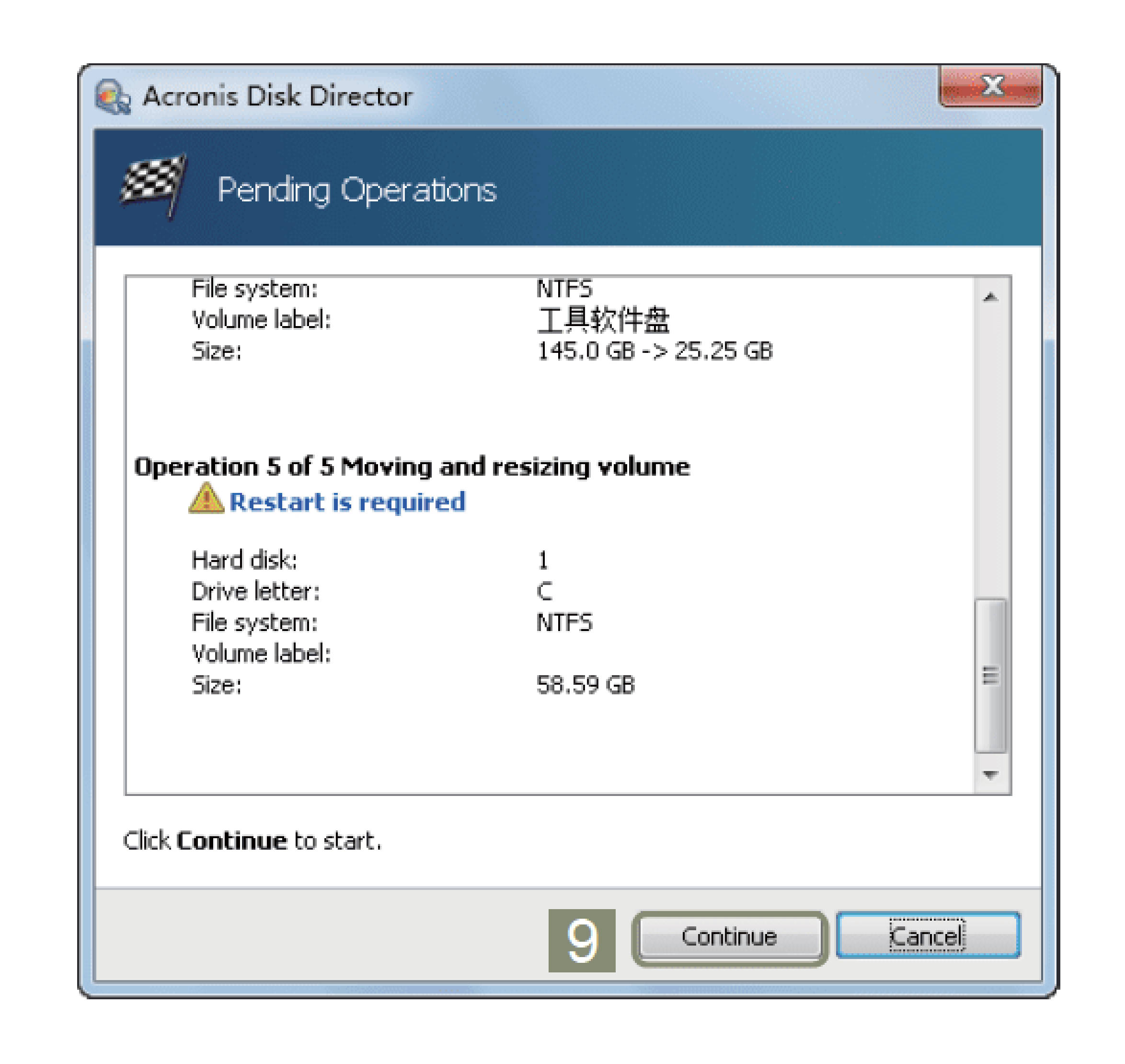


第4步：打开任务对话框

返回主界面中，在其任务栏中将出现用户创建的任务标签，单击该标签将打开任务对话框。

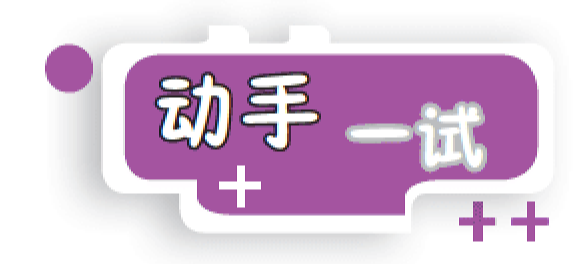
第5步：完成操作

软件将开始检测并分析其他各磁盘中的容量大小，然后提出方案，单击Continue按钮继续操作，完成后，在软件的主界面可以看到划分后C盘的空间将增大，再关闭软件重启电脑，即可完成C盘容量大小调整的操作。



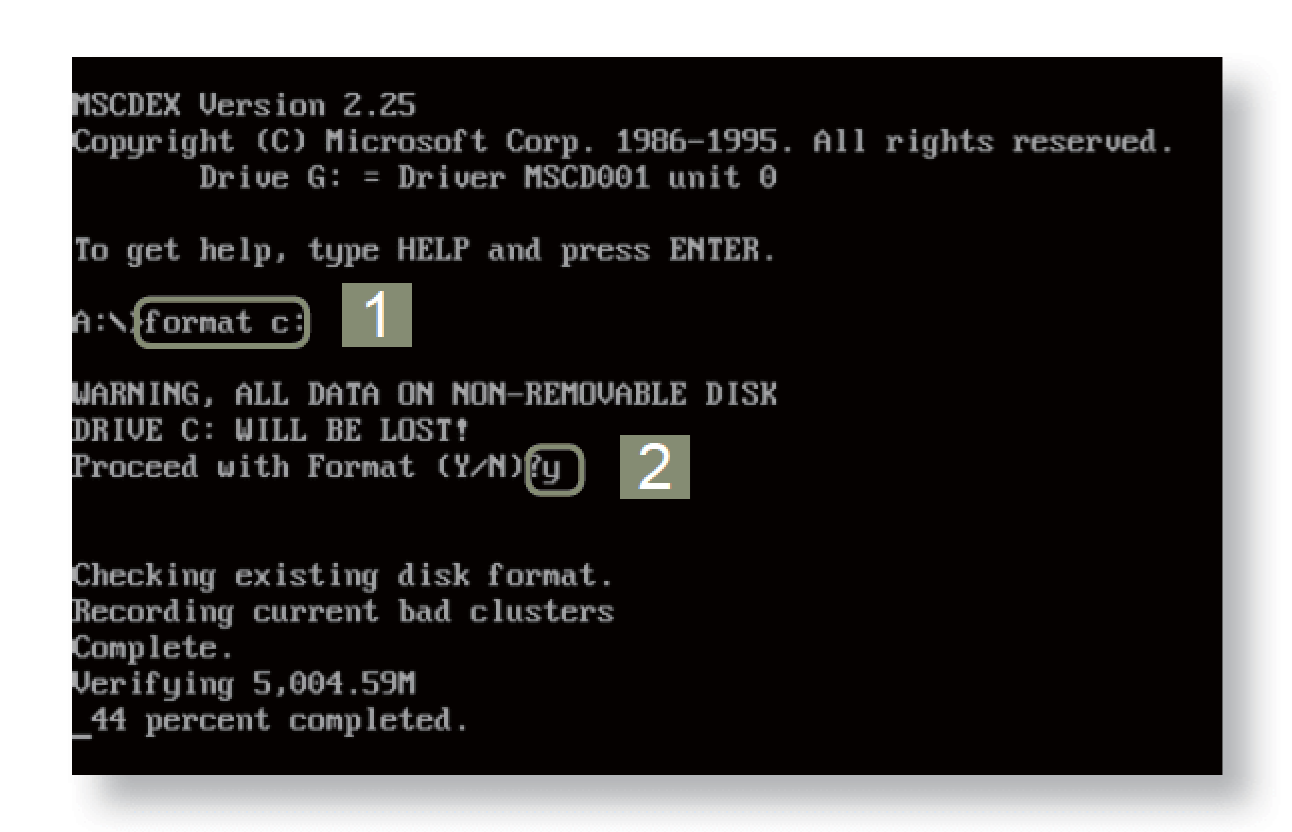
10.2.2 使用U盘启动重装Windows 7

在电脑中插入U盘，然后利用U盘启动进入DOS系统，便可在其中进行系统的重装，在重装系统前，应注意对系统中重要的数据进行备份。



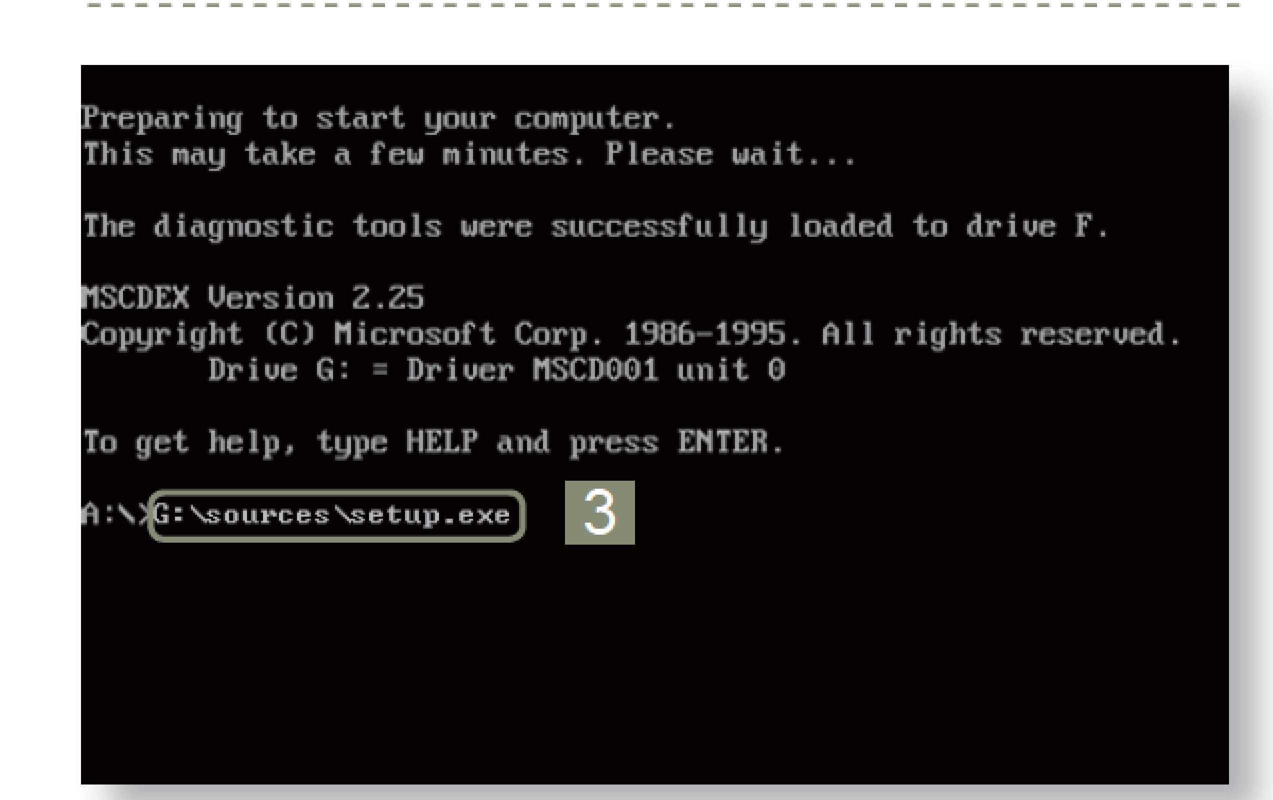
下面将在电脑中的C盘重装Windows 7操作系统，其具体操作如下。





第1步：格式化C盘

使用U盘启动盘进入DOS系统，在命令提示符后输入“format c：”，按Enter键，此时系统将询问是否删除C盘上的所有数据，输入“y”，按Enter键确认，系统开始格式化C盘，并显示格式化进度。



第2步：运行安装程序

当系统格式化完毕后，将Windows安装盘放入光驱中，然后在命令提示符后输入“G:\sources\setup.exe”，按Enter键，运行安装程序，系统开始复制文件。

第3步：设置安装选项并开始安装

文件复制完成后，在打开的窗口中设置系统的安装选项，这里保持默认，然后单击 下一步(N) 按钮，在打开的窗口中单击 现在安装(I) 按钮开始安装Windows 7。



第4步：接受许可条款

系统启动安装后，在打开的“请阅读许可条款”界面中选中“我接受许可条款”复选框，然后单击 下一步(N) 按钮，进入下一界面。



第5步：选择安装类型

在打开的“您想进行何种类型的安装？”界面中选择“自定义（高级）”选项。





第6步：选择要安装的位置

在打开的“您想将Windows安装在何处？”界面中选择“磁盘0分区1”选项（即C盘），然后单击下一步(N)按钮。

提示：用户可在列表框下方单击相应按钮对选择的分区进行相关操作。



第7步：完成安装

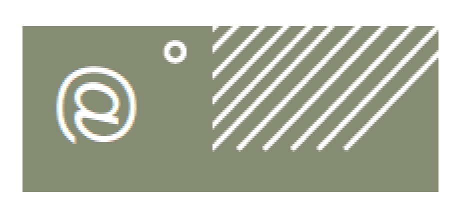
电脑将自动进行安装并显示安装信息，在此过程中电脑会进行多次重启操作，以完成相应的安装过程，安装完成后，系统将自动重启。

第8步：设置用户名和计算机名

在打开的对话框中输入要设置的用户名和计算机名称，这里将其设置为Lin和Lin-PC，然后单击下一步(N)按钮。

提示：在输入用户名时，其计算机名会自动添加。





为帐户设置密码

创建密码是一项明智的安全预防措施，可以帮助防止其他用户访问您的用户帐户。请务必记住您的密码或将其保存在一个安全的地方。

键入密码(推荐)(P):

再次键入密码(R):

键入密码提示(必需)(H):

我最想去的地方

请选择有助于记住密码的单词或短语。
如果您忘记密码，Windows 将显示密码提示。

13

14 下一步(N)

第9步：**输入用户密码和提示**

在打开的“为账户设置密码”界面中输入用户密码及密码提示，然后单击下一步(N)按钮。

提示：用户在输入密码时应注意密码的安全性，最好使用安全性高的密码。

新手解惑

Q：设置密码的作用是什么？

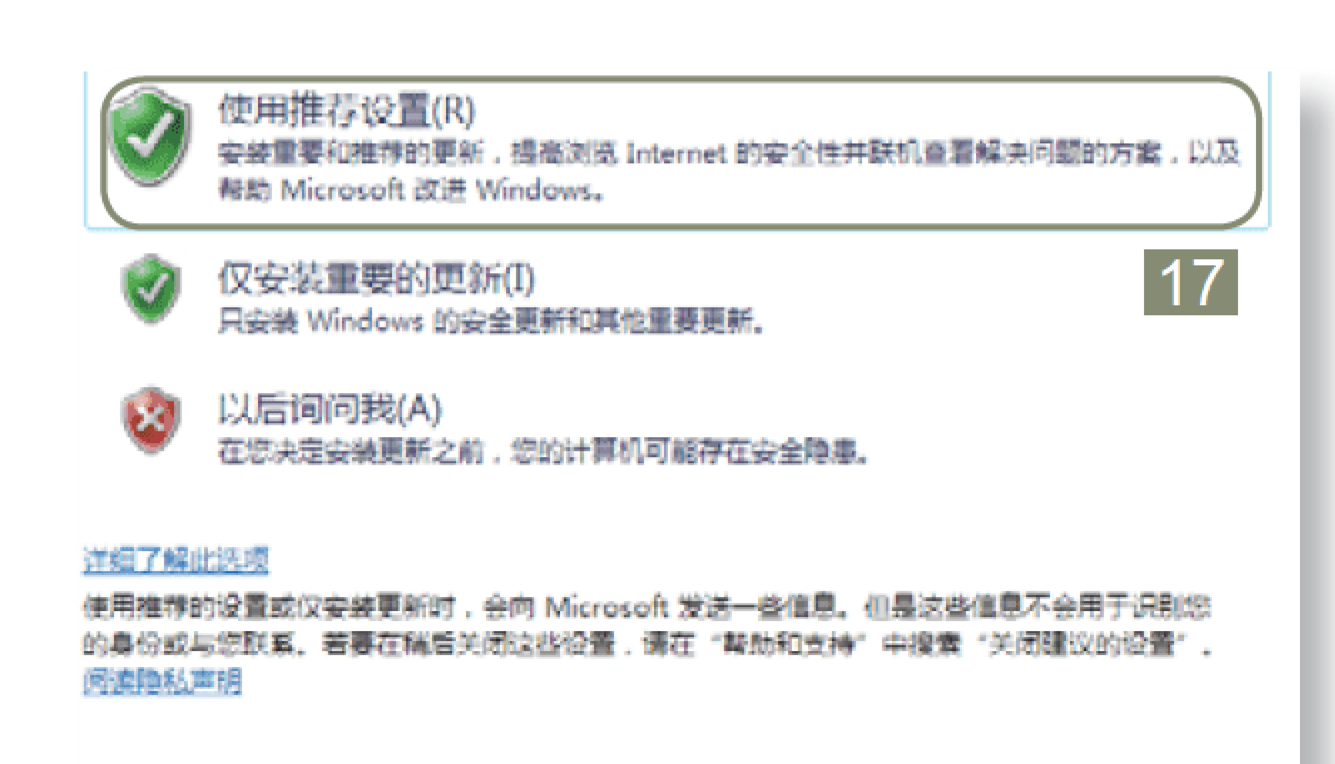
A：在登录Windows 7时需要输入该密码才能进入系统，因此必须牢记，而一个准确的密码提示有助于密码的记忆。

第10步：**输入密钥**

在打开的界面中输入产品密钥，然后选中“当我联机时自动激活Windows (A)”复选框，单击下一步(N)按钮。

提示：用户也可暂时不输入产品密钥直接进入下一步。





第11步：**设置自动更新**

在打开的“帮助您自动保护计算机以及提高Windows性能”界面中设置系统保护与更新，这里选择“使用推荐设置”选项。

第12步：设置日期和时间

在打开的“查看时间和日期设置”界面中设置正确的时区、日期和时间，这里将其设置为当前的时间和日期，然后单击下一步(N)按钮。

提示：用户在设置日期时只需确认系统默认的时间是否正确即可。





第13步：选择网络位置

在打开的“请选择计算机当前的位置”界面中设置电脑当前所在的位置，这里选择“工作”选项，完成后，系统将开始进行设置。



第14步：完成系统设置

在打开的界面中显示了设置的进度，完成个性设置后用户即可进入系统。

教你一招

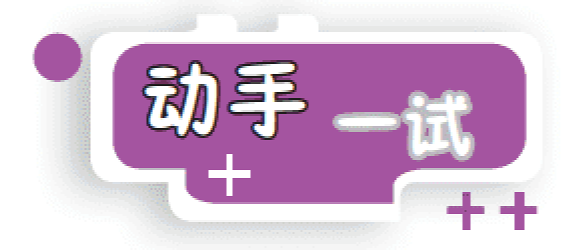
系统安装完成后的操作

完成系统的重装后，不要马上连接网线，应先安装杀毒软件后再接入网络进行系统漏洞的修复。

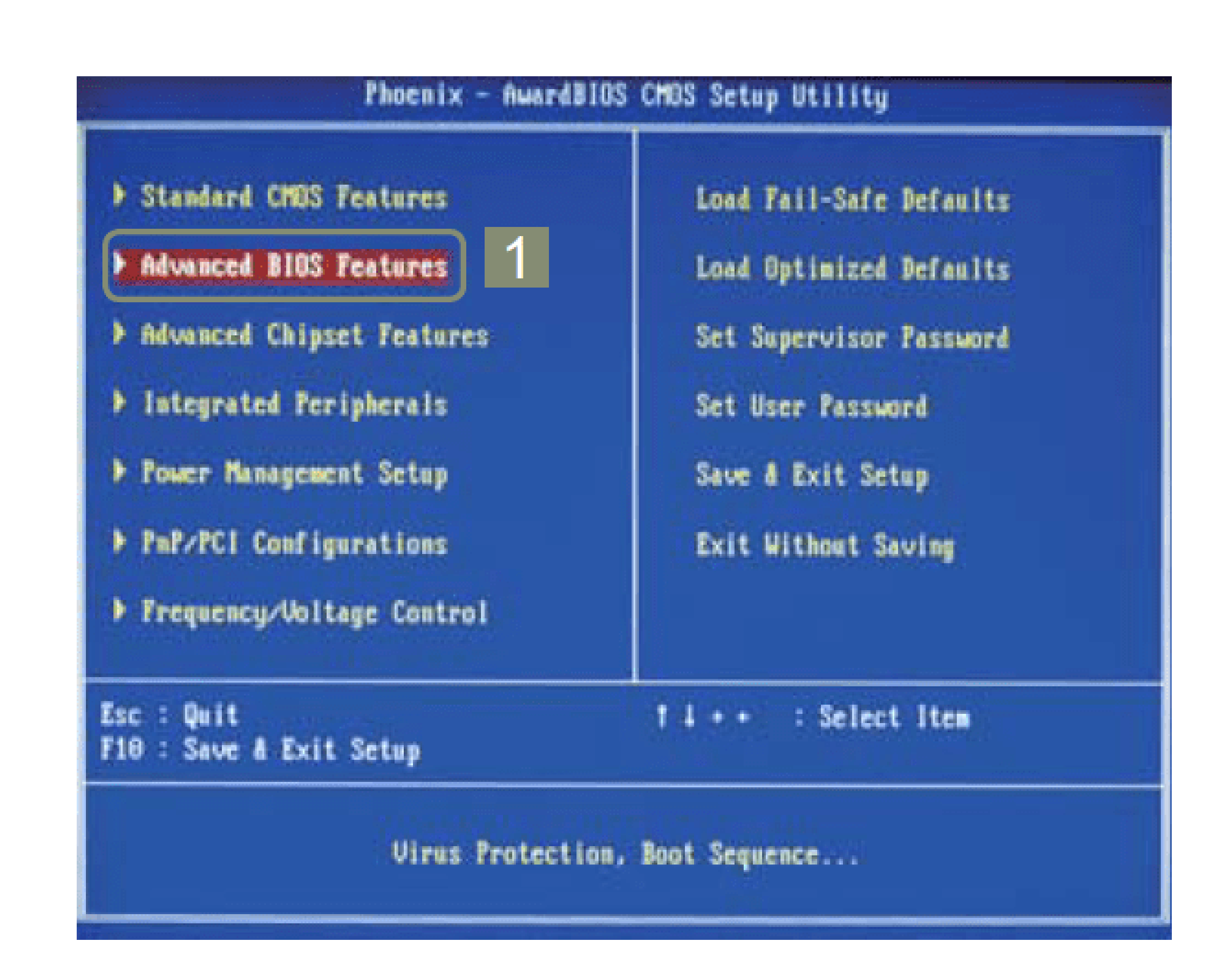


10.2.3 从光驱启动重装系统

通常用户在使用光盘为电脑安装操作系统时需设置从光驱启动电脑，这样就能引导操作系统的安装程序进行安装。



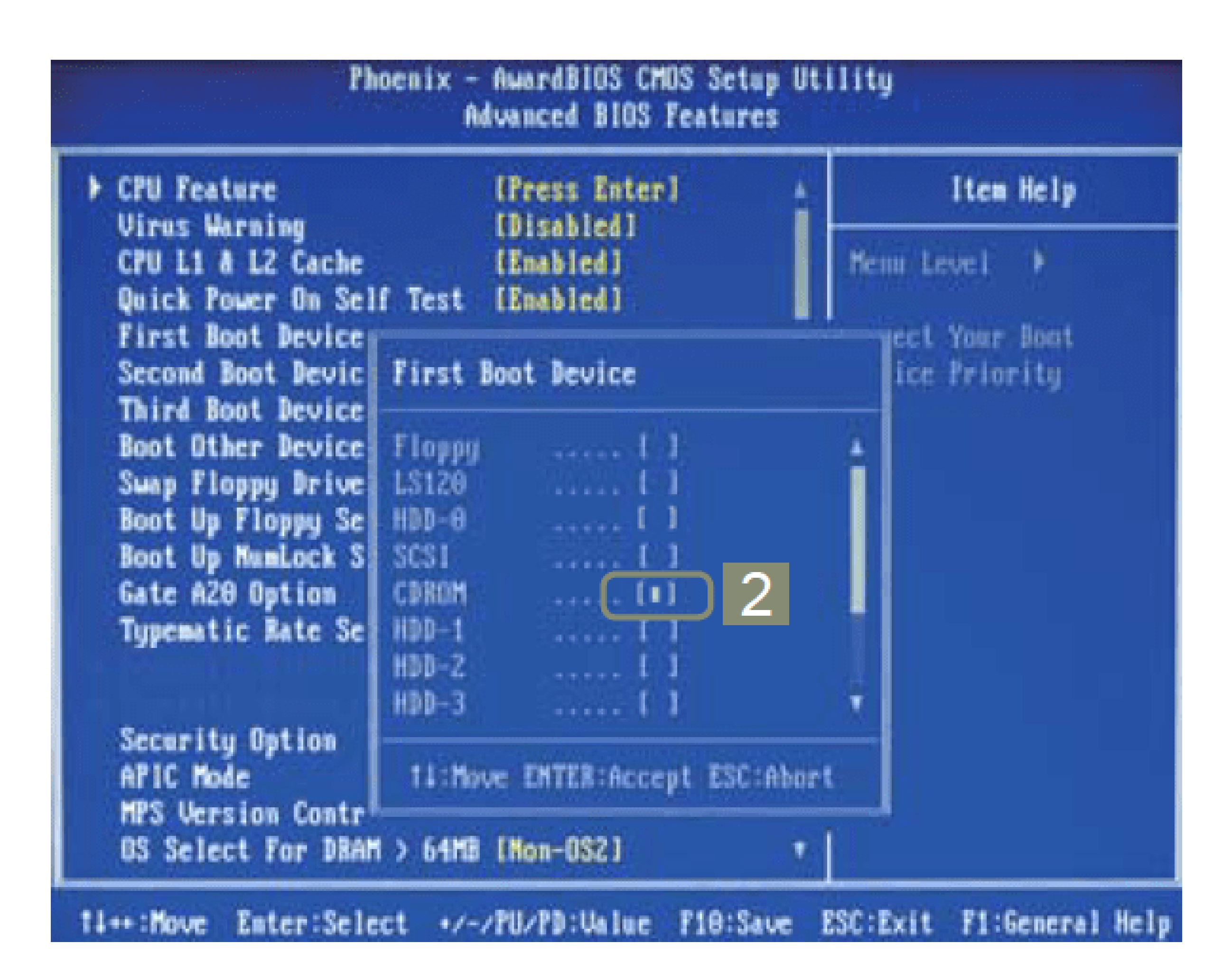
下面将启动电脑进入BIOS界面，在BIOS设置中设置电脑的第一引导器为光驱，其具体操作如下。



第1步：进入BIOS设置界面

启动电脑，按Delete键直到电脑进入BIOS界面，在该界面中选择Advanced BIOS Features选项，然后按Enter键进入。

提示：不同的主板进入BIOS的方式不同，通常台式机使用的主板直接按Delete键进入BIOS界面，而笔记本电脑进入BIOS界面大多数是按F2键。



第2步：设置第一引导设备

在进入的界面中选择First Boot Device选项，然后按Enter键，打开First Boot Device对话框，在其中选择CDROM选项，按Enter键即可确定所选选项。

新手解惑

Q：First Boot Device对话框中各设置选项的含义是什么？

A：Floppy选项：表示系统将从软驱引导。

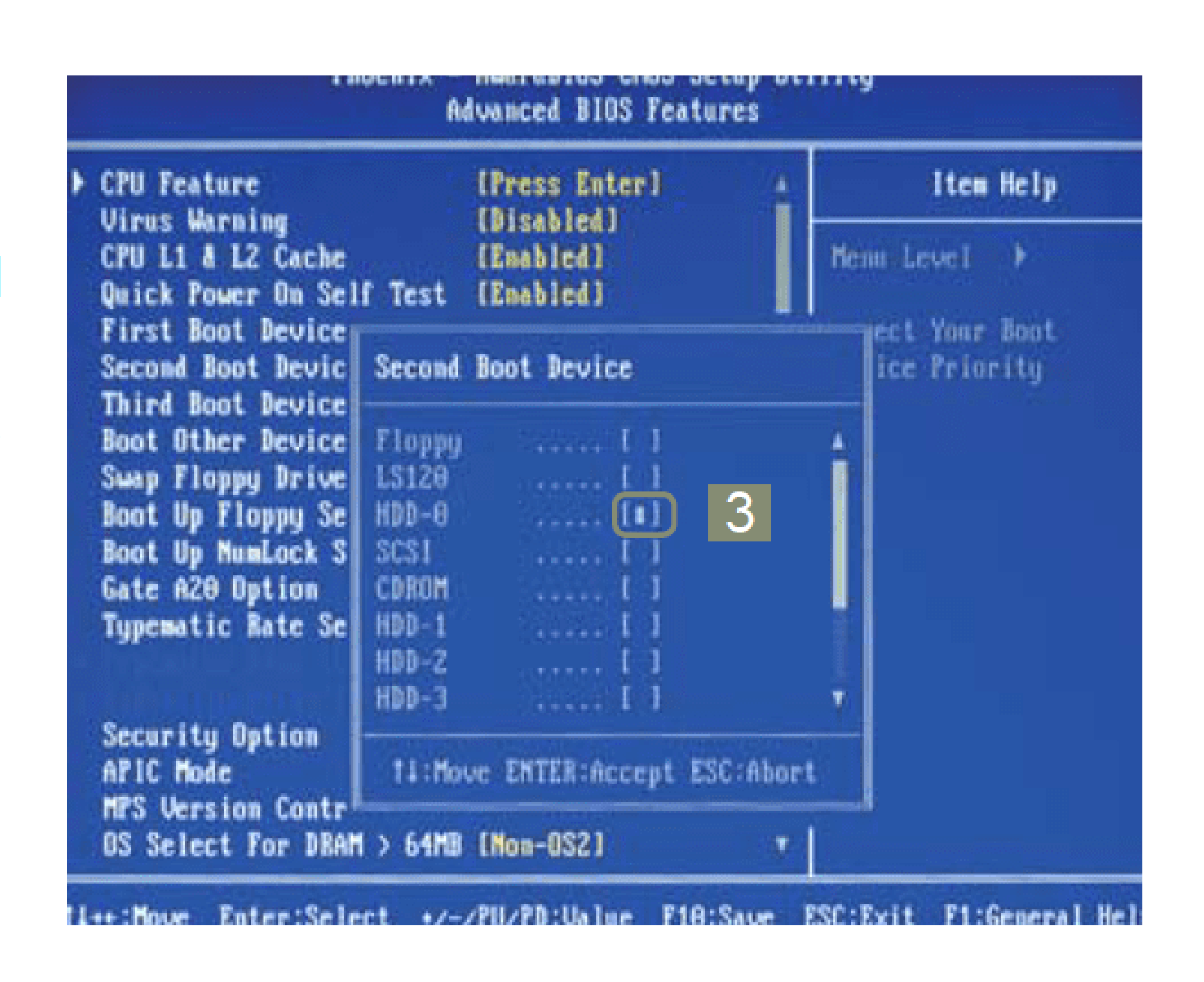
HDD选项：表示从硬盘引导，如电脑中存在多个硬盘，则该对话框中将显示为HDD-0、HDD-1和HDD-2等。

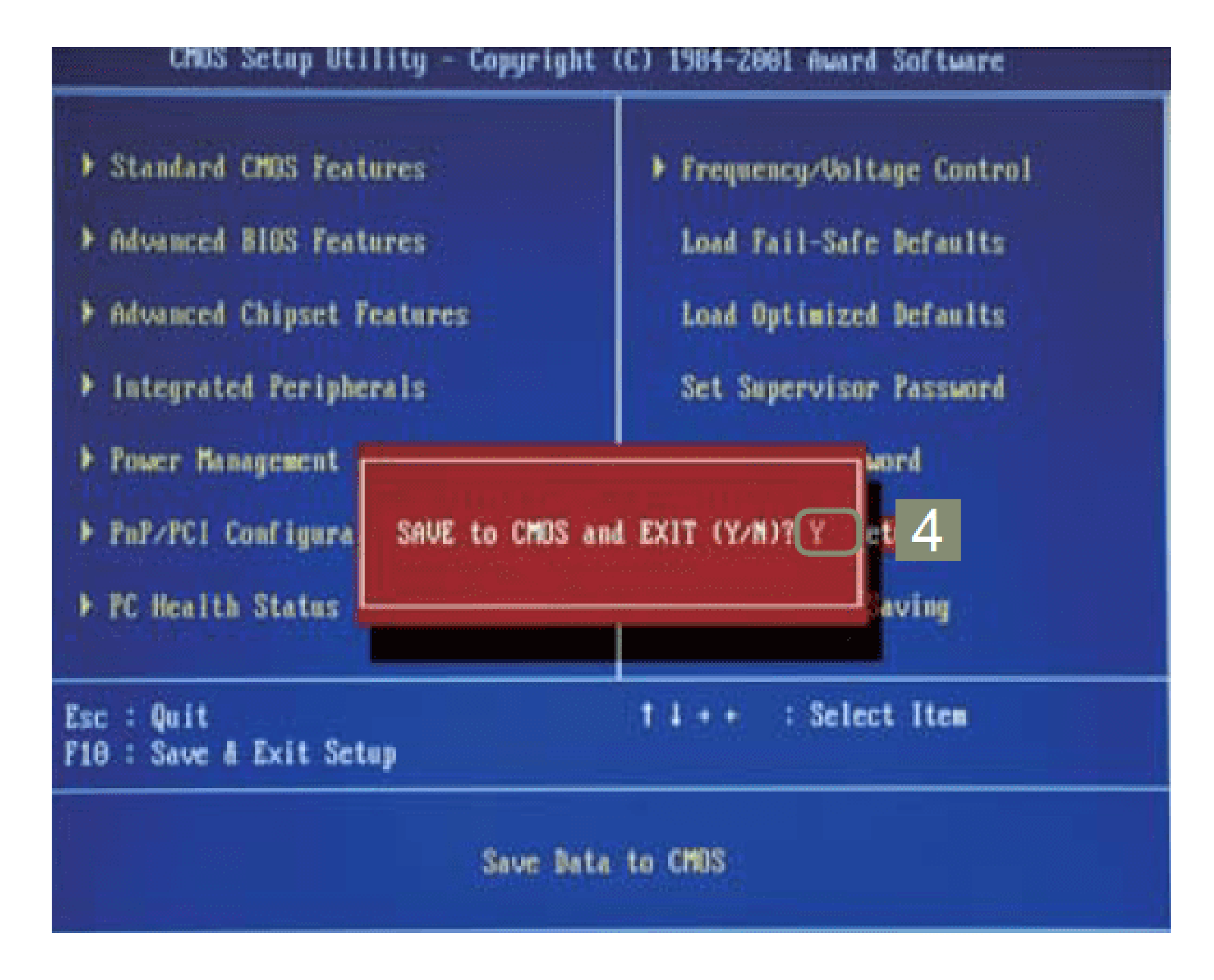
CDROM选项：表示系统从光驱引导。

第3步：设置第二引导设备

返回上一界面中，选择Second Boot Device选项，然后按Enter键，打开Second Boot Device对话框，在其中选择HDD-0选项，按Enter键确定所选选项。

提示：使用相同的方法将第三引导设备设置为HDD-1。





第4步：保存并退出设置

返回BIOS主界面，在其中选择SAVE to CMOS and EXIT选项，按Enter键即可打开提示框，然后在其中输入“Y”，按Enter键保存并退出BIOS界面。重启电脑后，即可从光驱启动电脑以便重装系统。

提示：还可按F10键保存并退出BIOS界面。

提示：设置完成后，即可放入安装光盘进行系统的安装，如光驱中不放入光盘，则系统会使用第2启动设备启动，即从硬盘启动。



跟我练习

娜娜要将电脑中的操作系统重装为Windows 7

任务1：使用USBoot软件制作U盘启动器，然后使用Acronis Disk Director 11 Home软件将系统盘重新调整。

任务2：使用光驱启动电脑，运行安装光盘安装Windows 7操作系统。



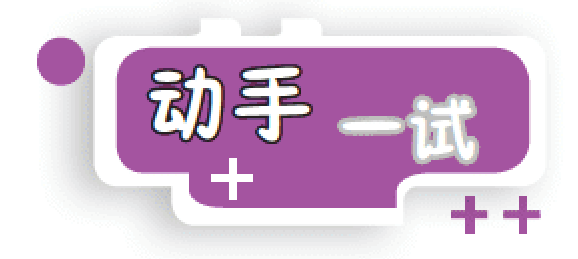


10.3 使用系统还原点

学习了系统重装后，尽管娜娜已经知道该怎样进行操作，但是她却感觉这太麻烦了，如果只是一些小问题，重装系统未免太小题大做了。于是她又找到阿伟，问：“有没有简单一点的操作啊，我可不想把时间浪费到这上面。”阿伟对她说：“当然，就是创建系统还原点，但这种方法是有限制的，必须进入系统才能使用。”

10.3.1 创建系统还原点

使用创建还原点的方法可将系统目前所处的状态进行保存，当系统遇到故障或更改了设置后出现异常现象，便可将其恢复。

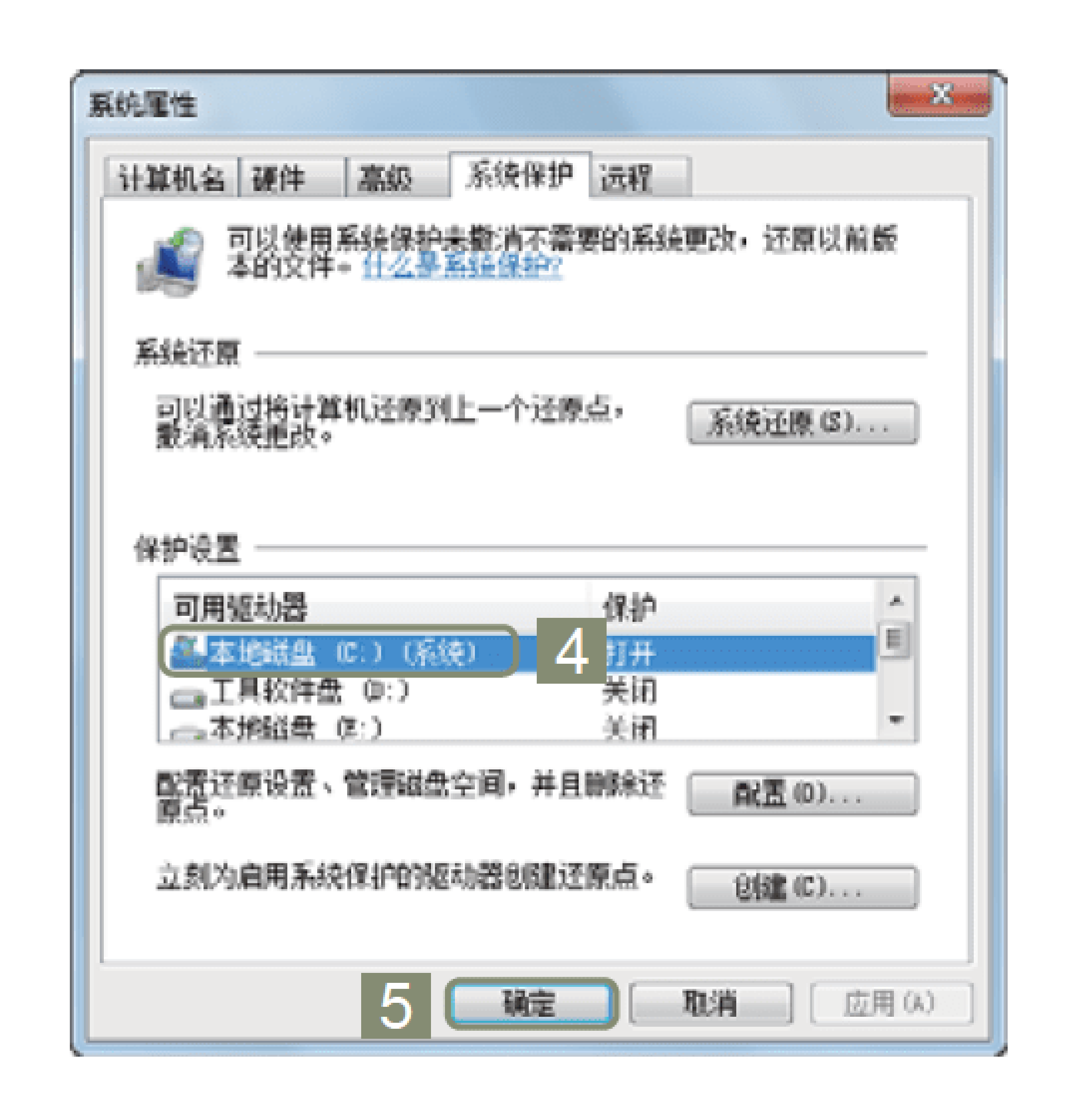


下面将使用系统自带的创建还原点功能以系统此时的状态创建一个还原点，其具体操作如下。



第1步：选择“创建还原点”选项

在桌面上单击按钮，在“搜索程序和文件”文本框中输入“backup”，在其上方将搜索出相关选项，这里选择“创建还原点”选项，打开“系统属性”对话框。



第2步：选择创建还原点的对象

在打开对话框的“系统保护”选项卡中的“保护设置”列表框中选择“本地磁盘（C：）”选项，然后单击 创建(C)... 按钮。

提示：在其中也可选择其他的驱动器来创建还原点。

第3步：设置还原点名称

在打开“创建还原点”对话框的文本框中输入要创建还原点的名称，这里输入“系统”，然后单击 创建(C) 按钮。

第4步：完成创建

在打开的对话框中将显示正在创建还原点，完成创建后，系统将打开提示对话框，在其中单击 关闭(O) 按钮即可。



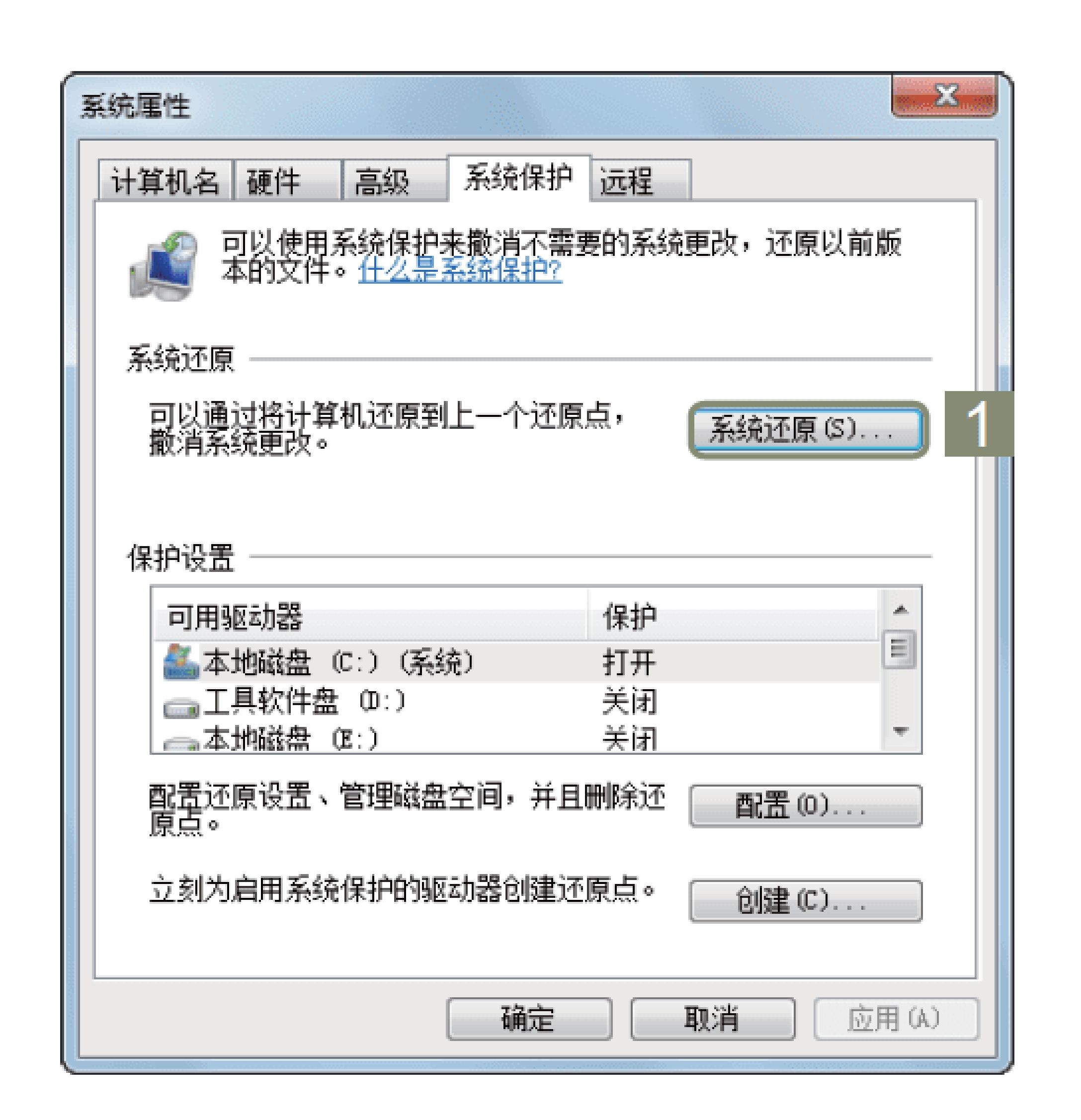


10.3.2 通过还原点还原系统

通过创建的系统还原点可以将系统还原到创建还原点前的状态，如果用户操作系统出现问题，可使用这种方法进行恢复。



下面将通过使用还原点的方法将系统进行还原，其具体操作如下。



第1步：打开系统还原向导

打开“系统属性”对话框，在其中的“系统保护”选项卡中单击 系统还原(S)... 按钮，打开“系统还原”向导。

提示：系统还原对话框也可通过右键单击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”命令打开。

教你一招

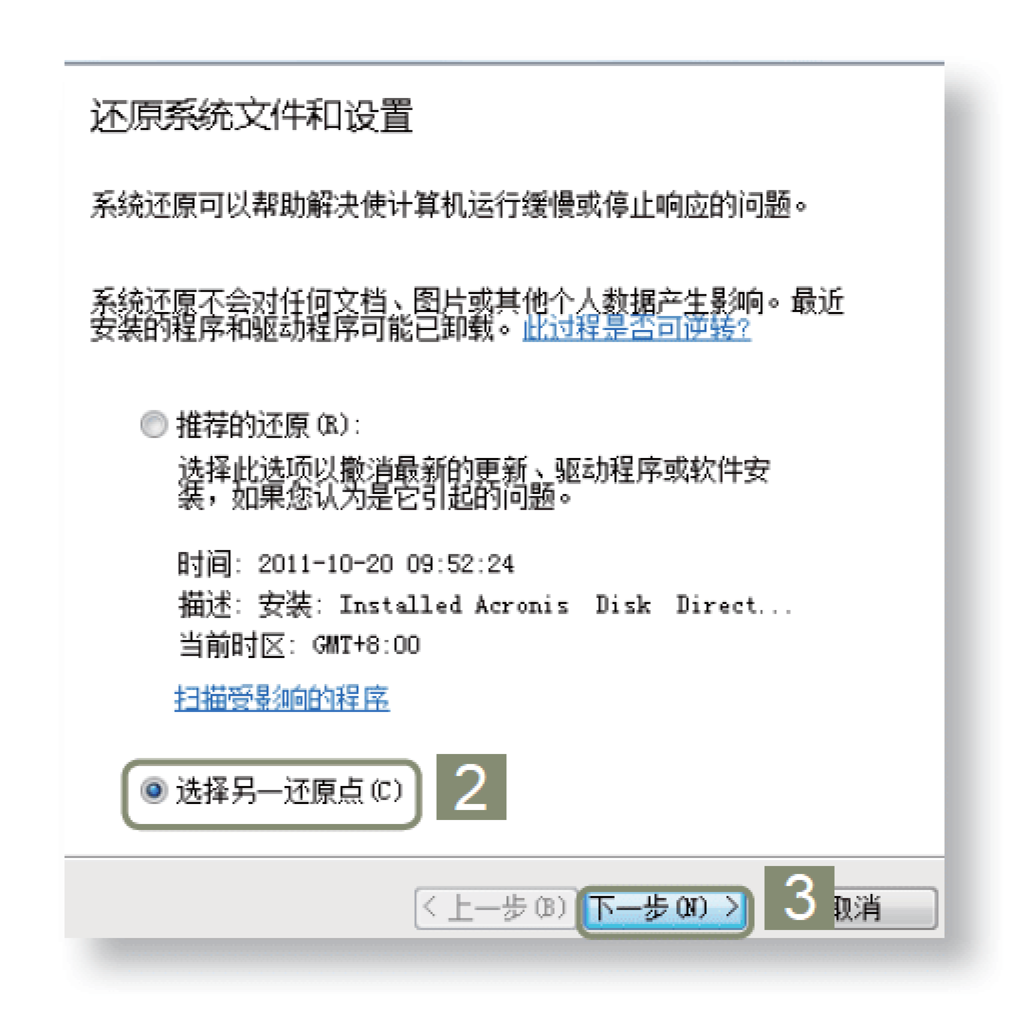
删除还原点

在该对话框中单击 配置(O)... 按钮，在打开对话框的“删除所有还原点”栏中单击 删除(D) 按钮，即可将系统还原点删除。

第2步：选择还原方式

在打开的“还原系统文件和设置”对话框中选中“选择另一还原点”单选按钮，然后单击 下一步(N) > 按钮。

提示：在其中可单击“扫描受影响的程序”超链接，在打开的对话框中将显示还原后要删除的程序。

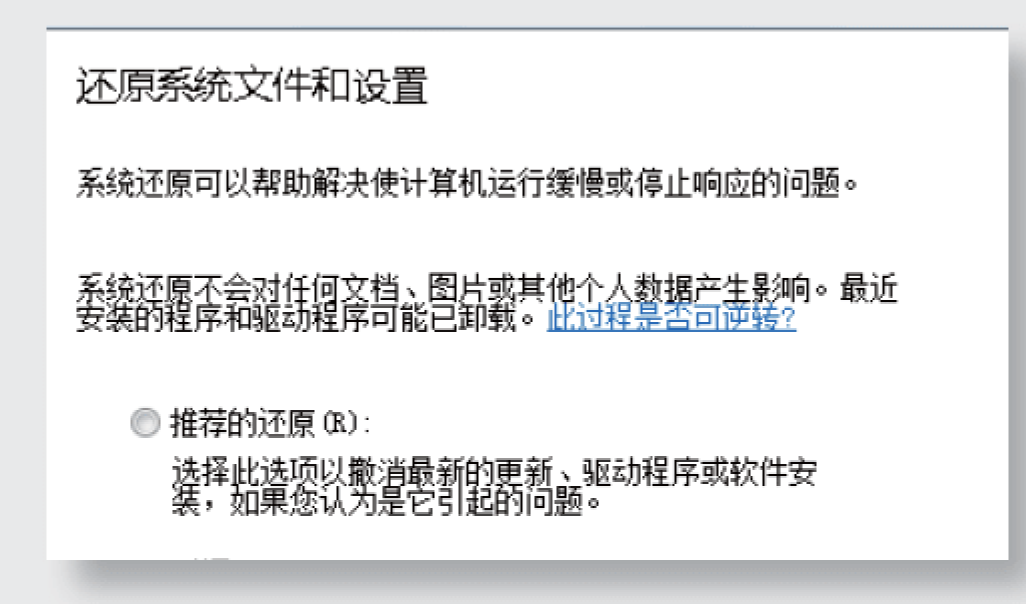


教你一招



使用推荐的还原点

在“还原系统文件和设置”对话框中选中“推荐的还原”单选按钮，系统将使用最近一次可能引起系统变更的还原点进行恢复。



第3步：选择还原点

在打开的“将计算机还原到所选事件之前的状态”对话框的“当前时区”列表框中选择“系统”选项，然后单击 扫描受影响的程序(A) 按钮，扫描还原后受影响的程序，扫描后单击 关闭(C) 按钮返回向导，单击 下一步(N) > 按钮确认选择。

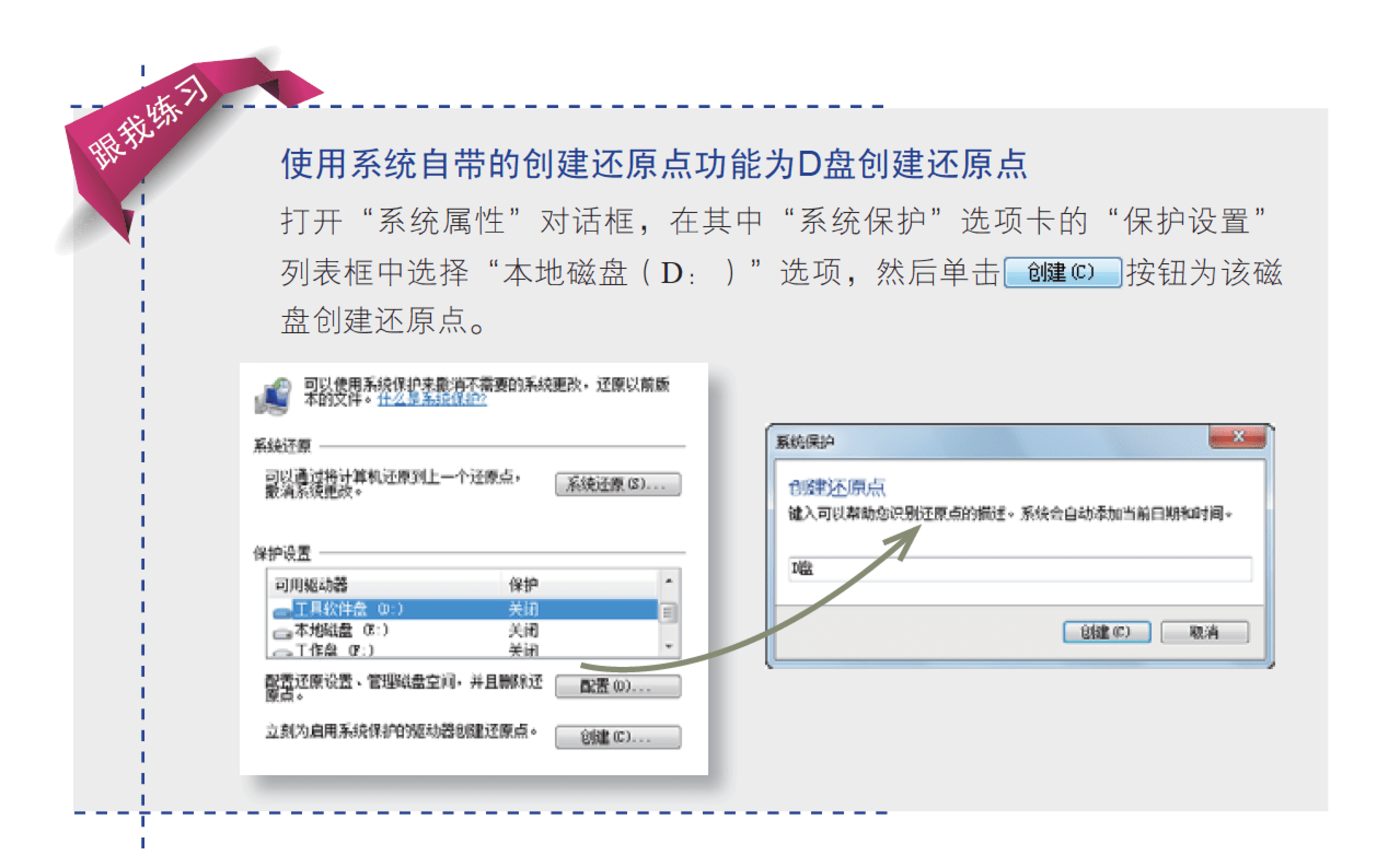


确认还原点
您的计算机将被还原到下面“描述”字段中的事件之前所处的状态。
时间：2011-10-20 15:51:30 (GMT+8:00)
描述：手动：系统
驱动器：本地磁盘 (C:) (系统)
扫描受影响的程序
如果您最近更改了 Windows 密码，则建议您创建密码重置盘。创建密码重置盘。
系统还原需要重新启动计算机才能应用这些更改。继续操作之前，请保存所有打开的文件并关闭所有程序。
< 上一步(B) 完成 7 取消

第4步：还原系统

在打开的对话框中将显示选择的还原点信息，并可在“驱动器”列表框中查看系统还原到的盘符，然后单击 完成 按钮开始系统的还原，还原后用户即可正常使用系统。





使用系统自带的创建还原点功能为D盘创建还原点

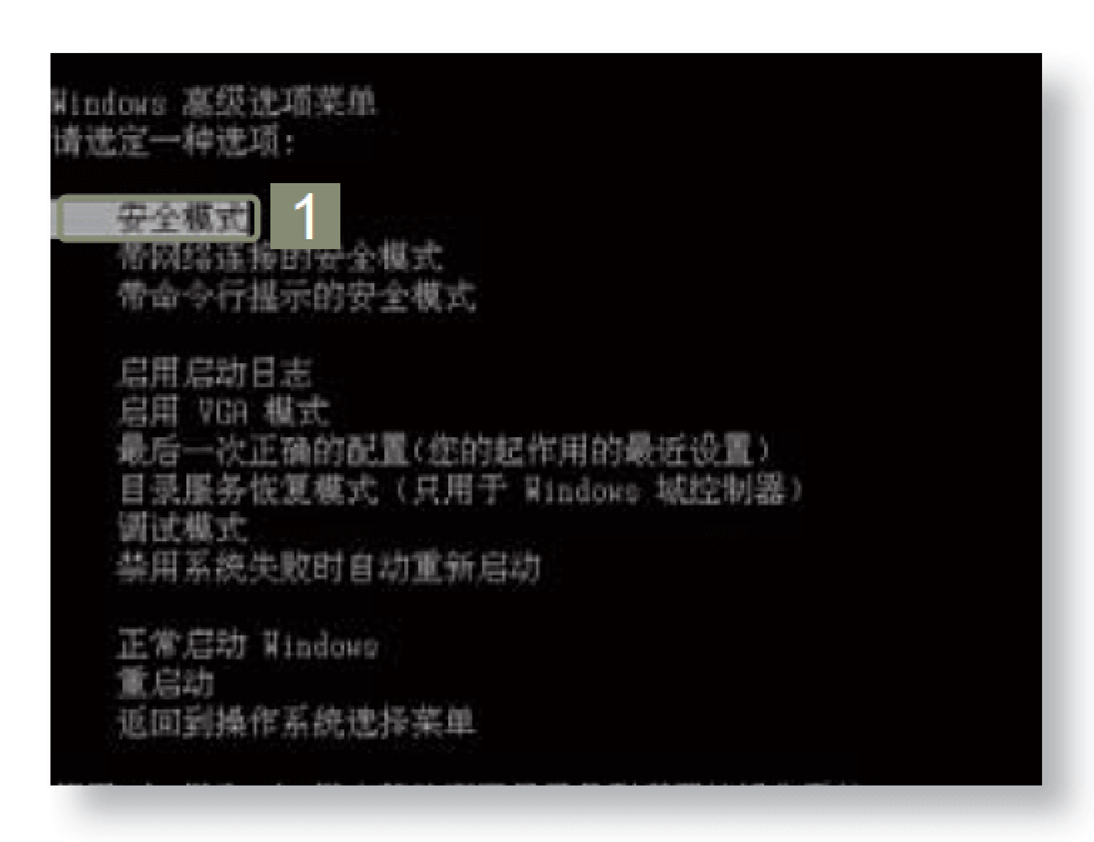
打开“系统属性”对话框，在其中“系统保护”选项卡的“保护设置”列表框中选择“本地磁盘（D：）”选项，然后单击 创建(C) 按钮为该磁盘创建还原点。

10.4 恢复系统文件

阿伟告诉娜娜：“如果Windows系统只是有少量的系统文件受损，那我们可以尝试使用Windows系统内置的SFC扫描修复命令，对已经遭受破坏的系统文件进行修复，如果修复成功，那Windows系统的启动又会恢复正常状态了。”娜娜听了阿伟的话以后很感兴趣，因为她终于可以不再去想备份和还原操作系统那样复杂的操作了，于是迫切地要求阿伟赶紧为她讲解。

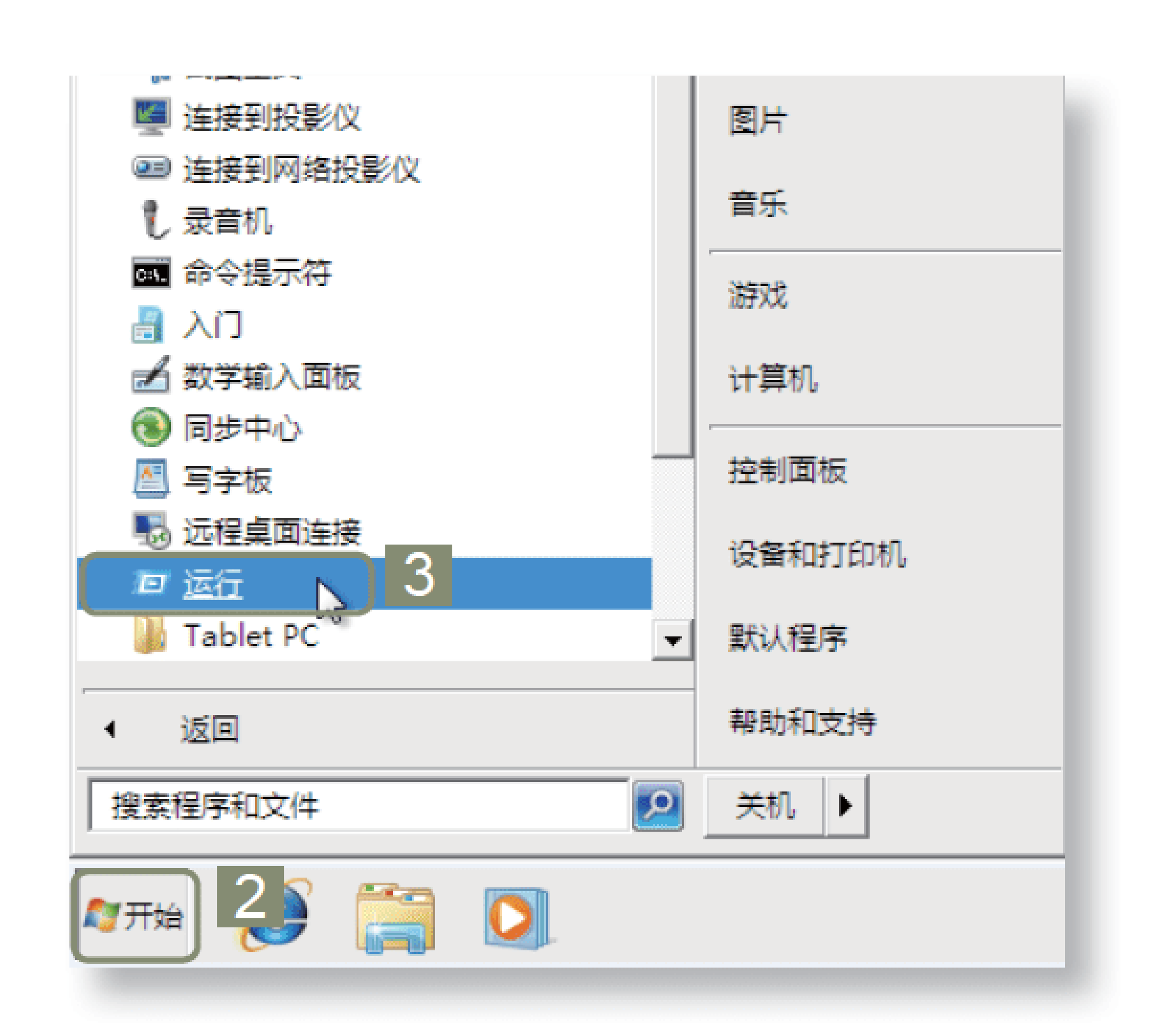


下面将对使用SFC命令恢复系统文件的方法进行讲解，其具体操作如下。



第1步：进入安全模式

启动电脑，按F8键进入“Windows高级选项菜单”界面，在其中选择“安全模式”选项，按Enter键进入电脑的安全模式界面。

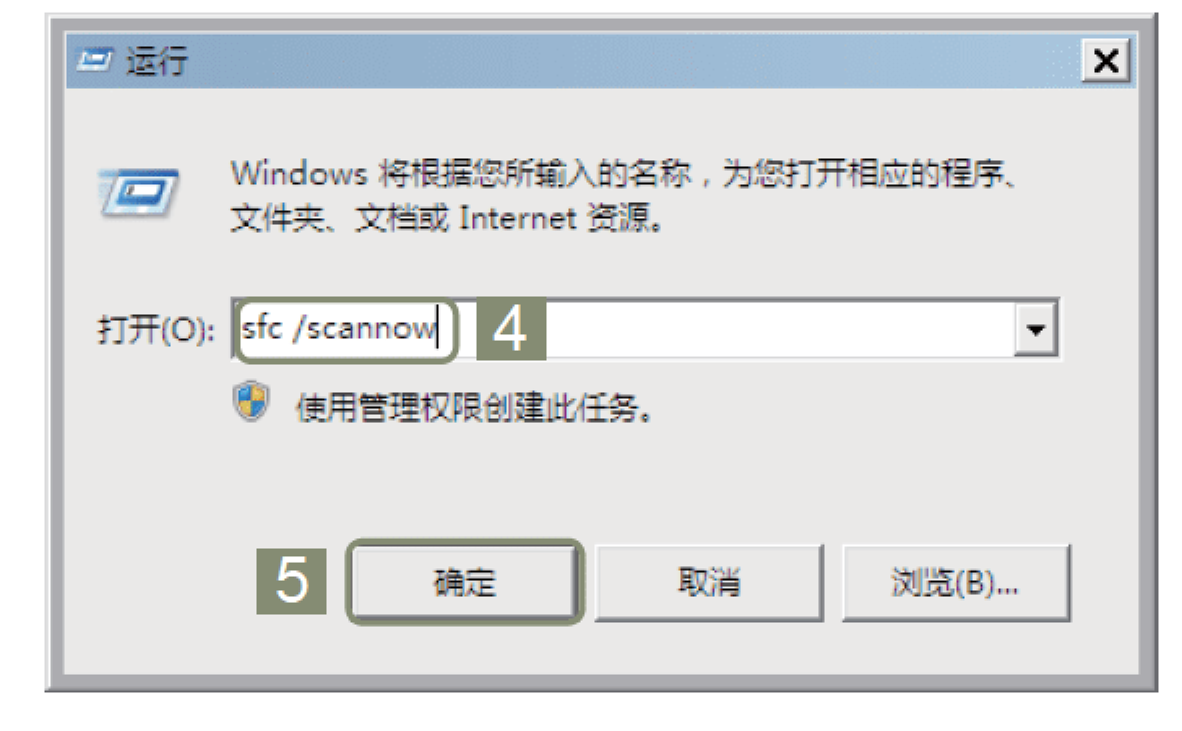


第2步：打开“运行”对话框

在安全模式界面中单击“开始”按钮，在打开的“开始”菜单中选择“所有程序”/“附件”/“运行”命令，打开“运行”对话框。

第3步：执行sfc命令

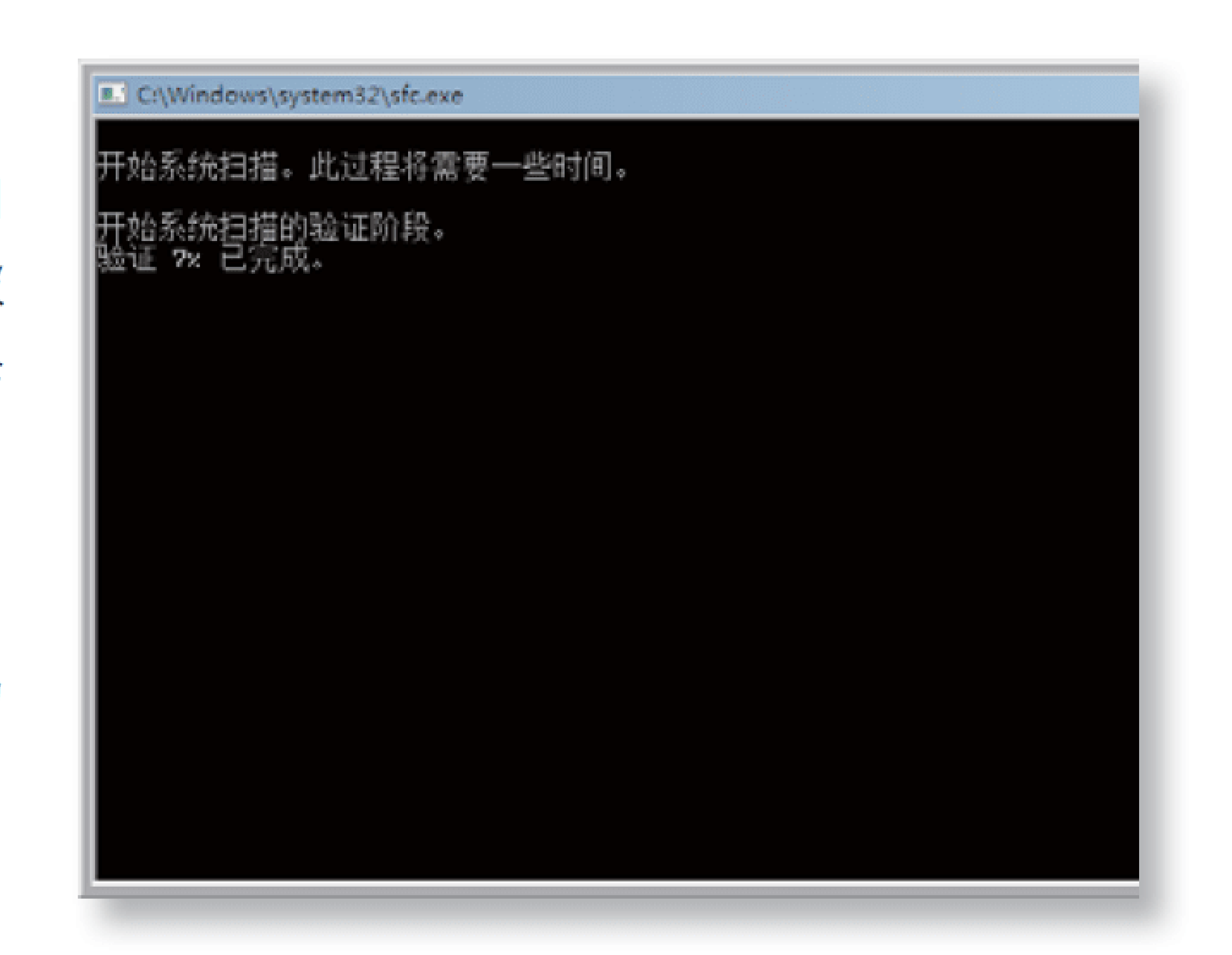
在打开对话框的“打开”下拉列表框中输入“sfc /scannow”命令，然后单击按钮，即可开始进行系统文件的扫描。



第4步：修复系统文件

在打开的窗口中将提示开始系统扫描并显示扫描的进度，在检查到被破坏的文件后，系统将进行自动修复，扫描完成后，该窗口将关闭。

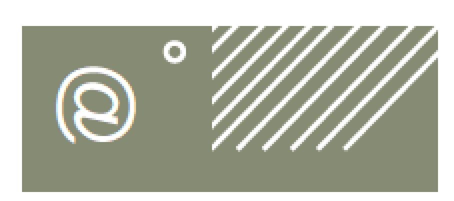
提示：执行该命令前将硬件系统盘放入光驱中，以便恢复受损的文件。

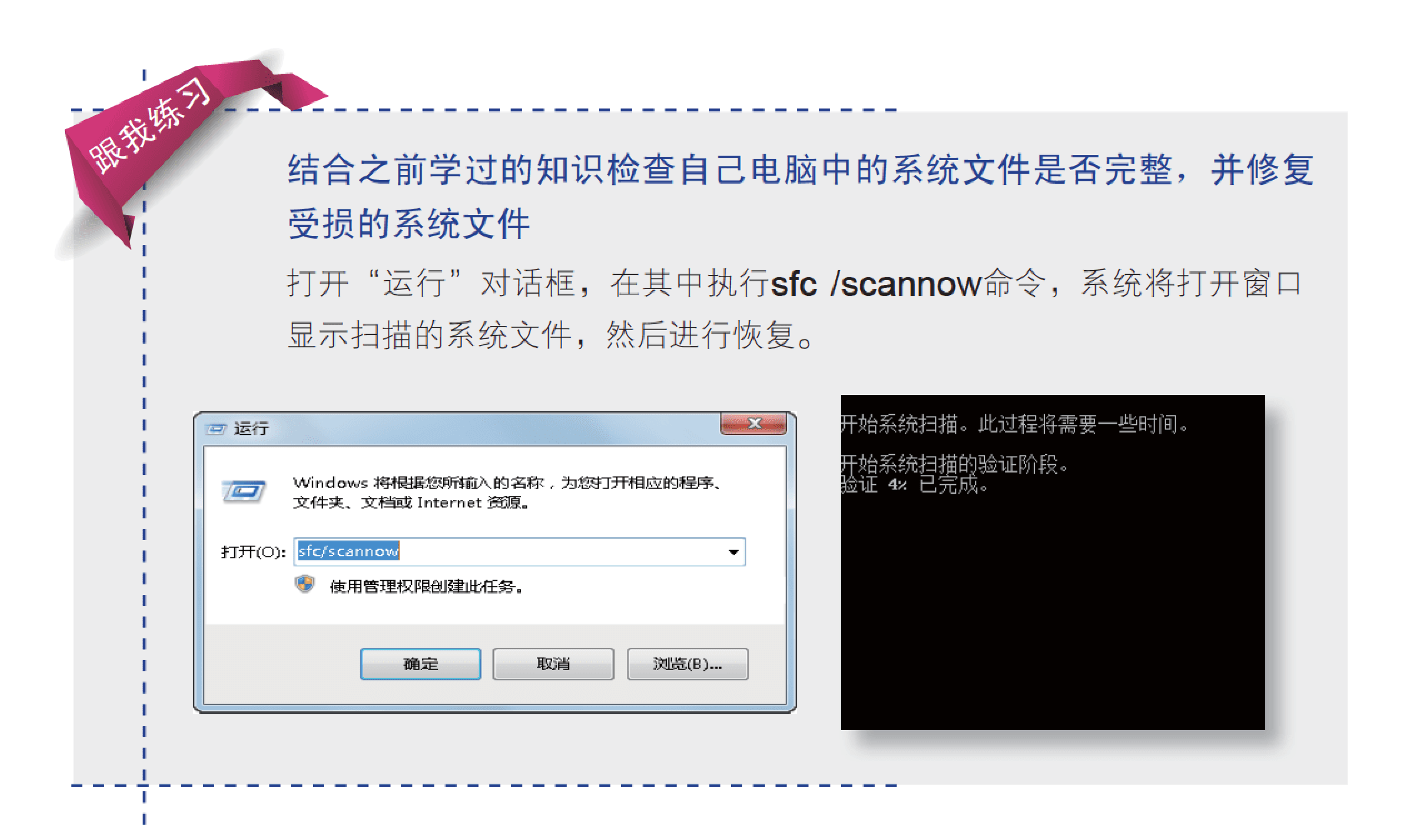


教你一招

使用安装光盘进行系统文件的修复

除此之外，用户还可使用安装光盘直接进行恢复系统文件，其方法为：使用光盘引导系统后，在进入安装向导后按R键即可开始系统的修复。





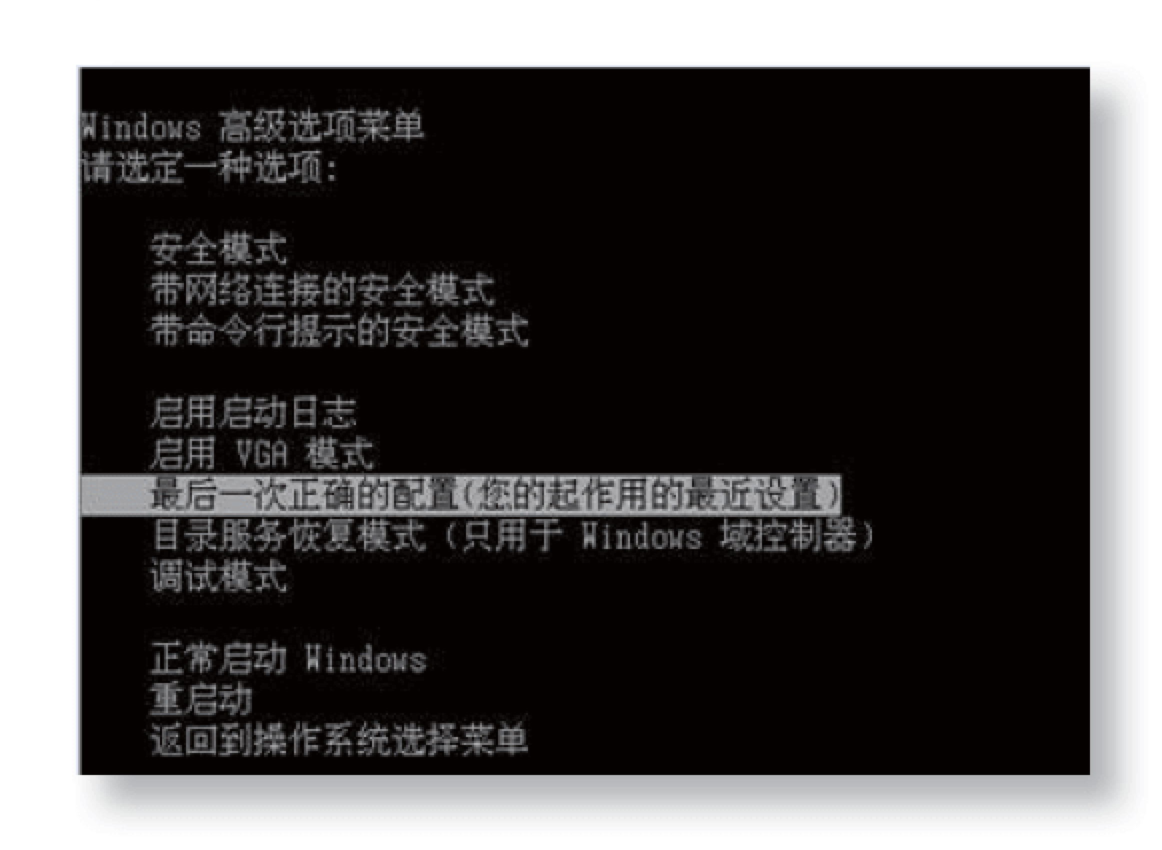
结合之前学过的知识检查自己电脑中的系统文件是否完整，并修复受损的系统文件

打开“运行”对话框，在其中执行sfc /scannow命令，系统将打开窗口显示扫描的系统文件，然后进行恢复。

10.5 更进一步——操作系统快速急救

通过前面的学习，娜娜已经掌握了操作系统的备份和还原等操作，并且她知道，要想不让自己后悔莫及，必须先做好操作系统的备份工作。今天娜娜又找到阿伟，因为她感觉阿伟还有一些特殊的技巧没有告诉她，于是对阿伟说：“我今天是来向你请教的，我知道对于操作系统的急救你很有经验，给我讲讲吧！”阿伟愣了一下，他没想到娜娜会主动向他请教问题，于是他很乐意地答应了。

第1招 恢复系统最后一次正确的配置



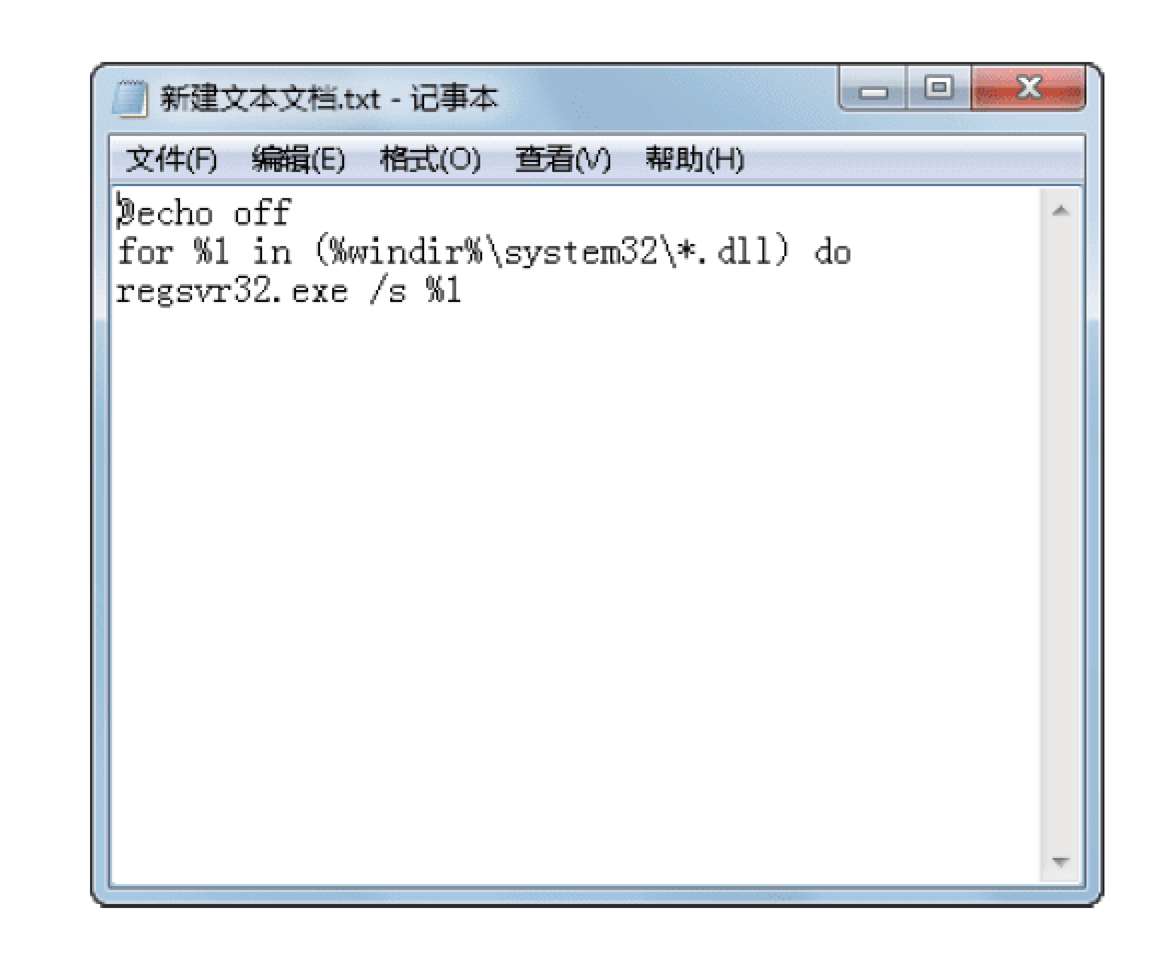
当系统因安装了一些软件而导致不能正常启动时，可使用最后一次正常启动的配置进行恢复，其方法如下：

①重新启动电脑，在进入系统加载前按F8键，进入系统启动菜单界面。

②在其中选择“最后一次正确的配置”选项，这样操作系统可能正常启动。

第2招 重注册DLL文件

由于系统DLL文件丢失引起Windows系统运行不正常故障时，不需重新安装操作系统，只需对已经丢失的DLL文件重新注册，就能让系统恢复正常运行状态。其方法如下：



①在桌面上新建一个文本文档，并在其中输入“@echo off for %1 in (%windir%\system32*.dll) do regsvr32.exe /s %1”文本，将其以“.bat”格式保存。

②双击该文件，即可重新注册DLL文件，然后重启操作系统。

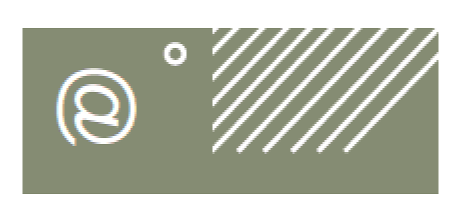
提示：Windows系统之所以会频繁受到损伤，主要是许多应用程序常常共享调用DLL文件，一旦有的应用程序在使用完毕被自动卸载后，这些应用程序所调用的DLL文件也会被删除，导致错误现象发生。

第3招 注销当前用户

如Windows系统的受损只是由于安装了不恰当的软件或对软件进行了设置而导致，那么可通过“注销当前用户”的方法，来对受损的Windows系统进行急救，由于软件对系统设置的影响往往只能限于当前登录的用户，在当前用户状态下系统不能正常运行，可注销当前用户，并以其他的用户重新登录系统，这样Windows又能恢复正常运行状态。



提示：在注销当前用户前，如系统中不存在其他用户，则需创建一个新的用户账户。



第4招 设置系统配置

在Windows 7操作系统中，可设置引导系统选项，以提高系统相关硬件的利用率，使系统安全运行，其方法如下：

①单击按钮，在搜索程序文本框中输入“msconfig”，打开系统配置窗口，选择“引导”选项卡，在其中单击 高级选项(V)... 按钮。

②在打开的“引导高级选项”对话框中选中“处理器数”复选框，在其下拉列表框中选择2选项，然后选中“最大内存”复选框，在其数值框中输入电脑的内存容量，重启电脑即可。



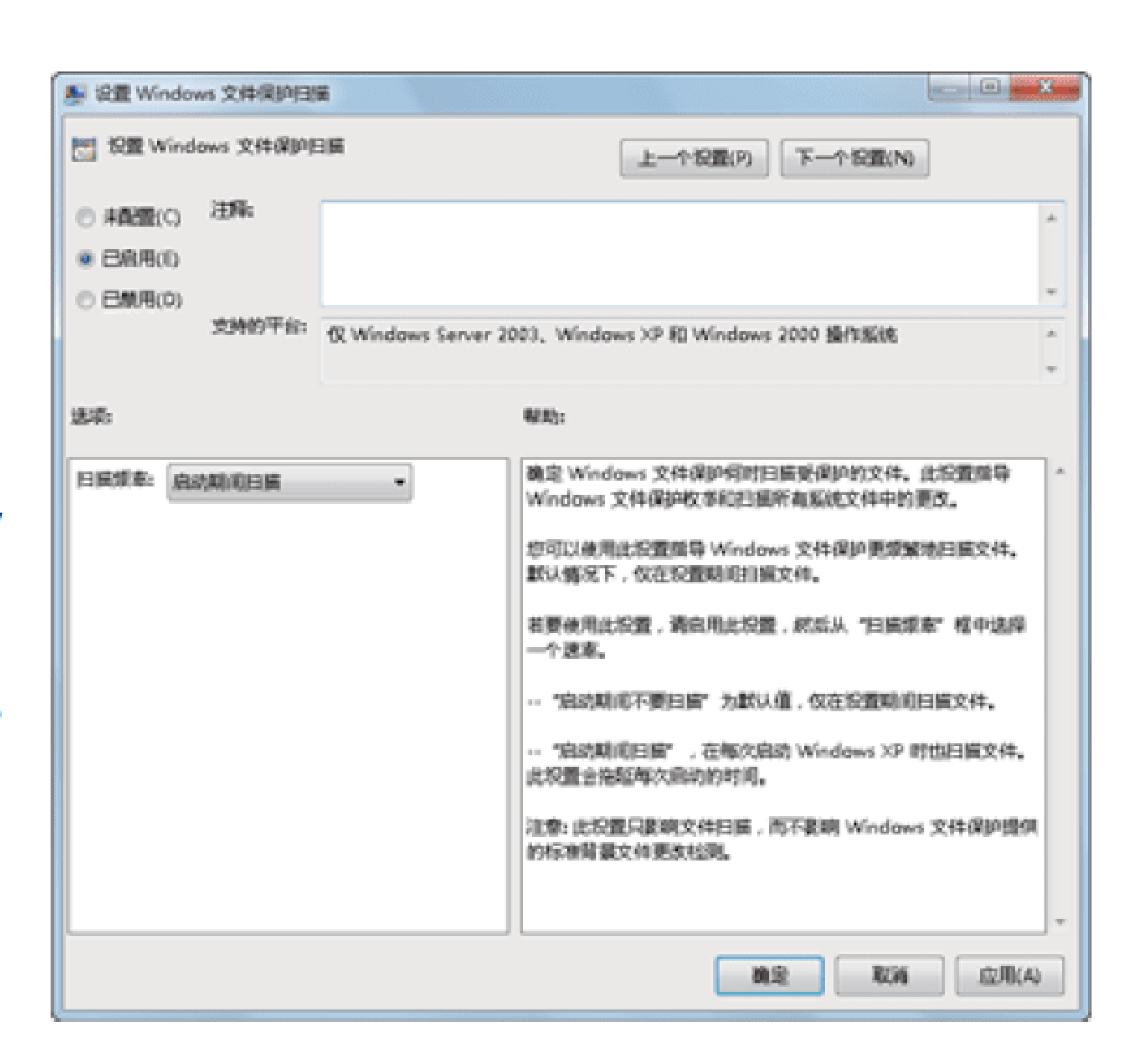
提示：在“引导高级选项”对话框中选中相应的复选框时，在其下拉列表框或数值框中将根据电脑的实际配置显示相应的数据。

第5招 设置Windows文件保护扫描

用户可在组策略中设置自动扫描系统文件，以保证操作系统的正常运行，其方法如下：

①在“运行”对话框中执行gpedit.msc命令，打开组策略，在其中依次展开“计算机配置/管理模板/系统/Windows文件保护”选项。

②在右侧窗格中双击“设置Windows文件保护扫描”选项，在打开的对话框中选中“已启用”单选按钮，然后单击 确定 按钮即可。



10.6 活 学 活 用

（1）在电脑中安装MaxDOS软件，并重启电脑进入软件界面使用MaxDOS对系统进行备份。

（2）使用USBoot软件制作U盘启动，并进入BIOS界面，在BIOS界面中设置系统从U盘引导。

（3）使用U盘引导系统重装Windows 7操作系统。

（4）利用Windows操作系统的系统保护功能为电脑C盘创建还原点。

（5）使用系统安装光盘修复系统文件，通过在“运行”对话框中执行命令和设置从光驱启动两种方式进行。



- ☑ 想知道电脑为什么会自动重启吗？
- ☑ 还在为电脑突然蓝屏而烦恼吗？
- ☑ 想知道怎样处理电脑故障而不必重装系统吗？
- ☑ 浏览器故障还在困扰着你吗？



第 11 章 典型电脑故障急救

娜娜通过阿伟这段时间的帮助，对电脑安全方面的知识掌握了不少。但她却觉得阿伟教给她的知识很多都是有关防御的，而关于具体故障处理的知识却没讲多少，于是她又找到阿伟，让阿伟给她补补这方面的知识。阿伟弄明白娜娜的来意后，对她讲道："电脑可能出现的故障有很多，我就给你讲讲平常可能遇到的比较典型的故障吧！"

11.1 操作系统自动重启

阿伟告诉娜娜，在使用电脑的过程中，经常会遇到电脑自动重启的现象，这带来最直接的危害就是在使用过程中用户的资料会因电脑的自动重启而丢失。娜娜对这感觉很好奇，于是就问阿伟：“电脑出现自动重启的原因是什么呢？我们又该如何来解决？”阿伟接道：“先别着急，下面我慢慢来为你讲解。”

11.1.1 电脑自动重启的原因

电脑自动重启是什么原因，这是让许多用户都经常发愁的事情，通过网络可以寻找到电脑自动重启的原因，但是由于电脑知识不足，很难判断出自己电脑具体是由什么原因引起的。电脑重启的原因可以从软件、硬件以及外界影响等方面来进行分析。

新手解惑

Q：电脑自动重启主要包括哪些方面的原因？

A：软件方面：病毒、系统文件被破坏和计划任务的设置。

硬件方面：电源电压不稳定、内存与插槽的接触不良、电源插座接触不良、CPU温度过高以及硬件不兼容。

外界原因：电压不稳定、强磁干扰以及灰尘太多。

1. 软件方面

系统中软件的一些故障会导致自动重启，如病毒的影响、系统文件受损以及相关的计划任务软件的作用等。



下面将介绍由于软件原因（病毒、系统文件和计划任务影响）引起的电脑自动重启现象。



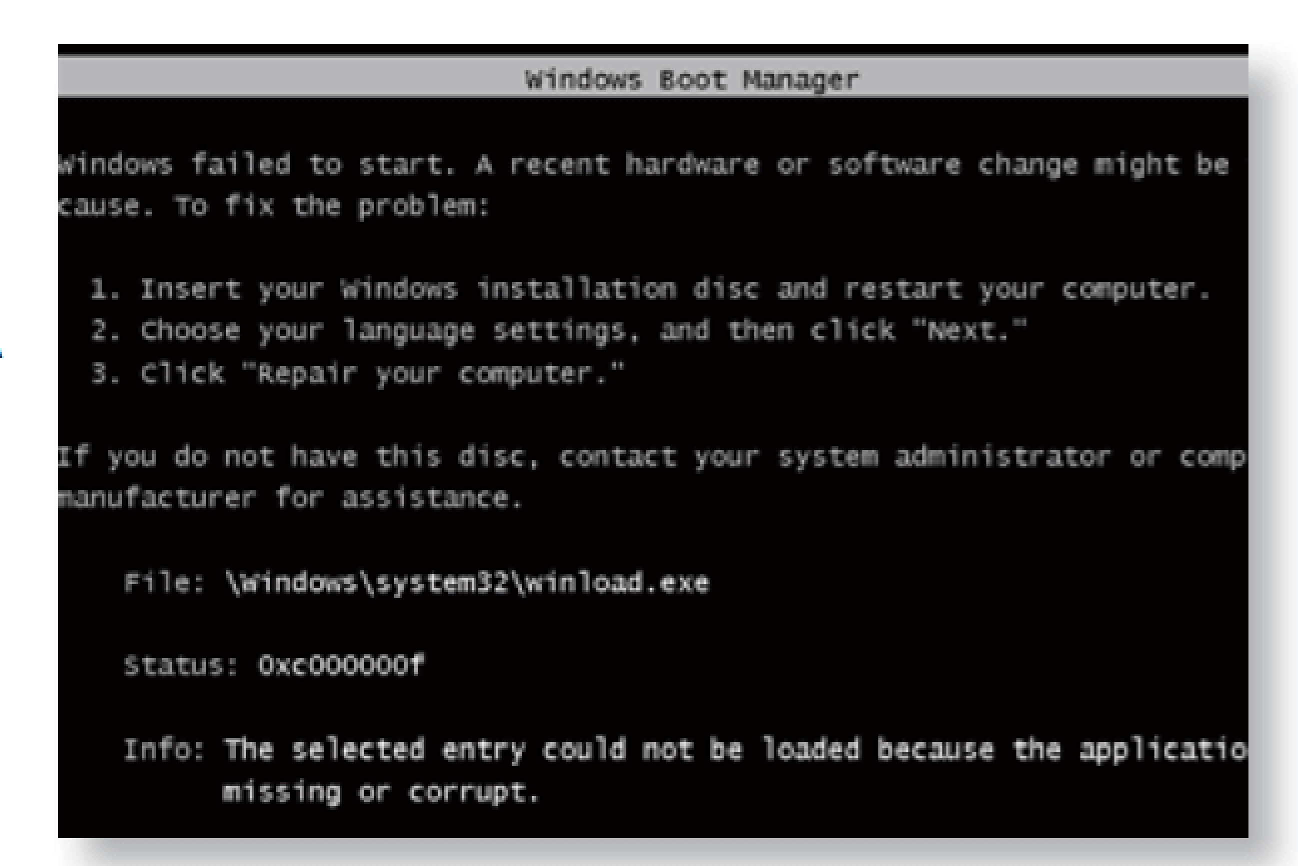
原因1：病毒导致

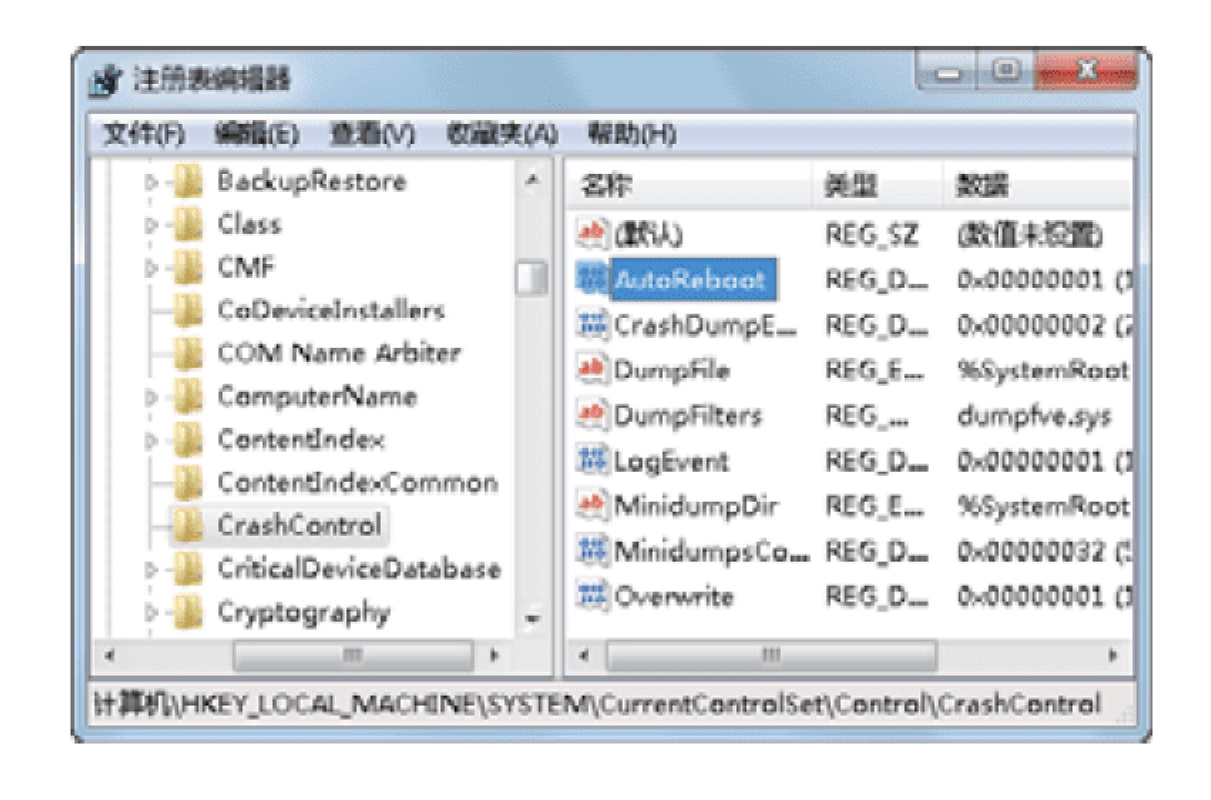
具体分析：如果电脑感染“冲击波”病毒，当其发作时会提示系统将在60秒后自动重启。该病毒程序可以从远程控制电脑的一切活动，包括让电脑重新启动。



原因2：系统文件损坏

具体分析：系统文件被破坏，如Windows 7中WINDOWS\SYSTEM32\CONFIG\SYSTEM目录下的系统文件被破坏，系统在启动时会因为无法完成初始化而反复重新启动。





原因3：计划任务软件的作用

具体分析：在注册表中或通过软件设置了电脑自动重启，且定时时刻到来时，电脑将会再次启动。对于这种情况，可打开启动项，检查里面有没有不熟悉的执行文件或其他定时工作程序，将其屏蔽后再开机检查。

2. 硬件方面

引起电脑重启的原因有多种，除了软件方面的原因外，硬件的相关问题同样会导致电脑自动重启。



下面将对由电脑硬件方面引起电脑自动重启的原因分别进行介绍。

原因1：电源问题

具体分析：劣质的电源不能提供足够的电量，因此，当系统中的设备增多、功耗变大时，劣质电源输出的电压就会急剧降低，最终导致系统工作不稳定，出现自动重启现象。

原因2：内存出现问题

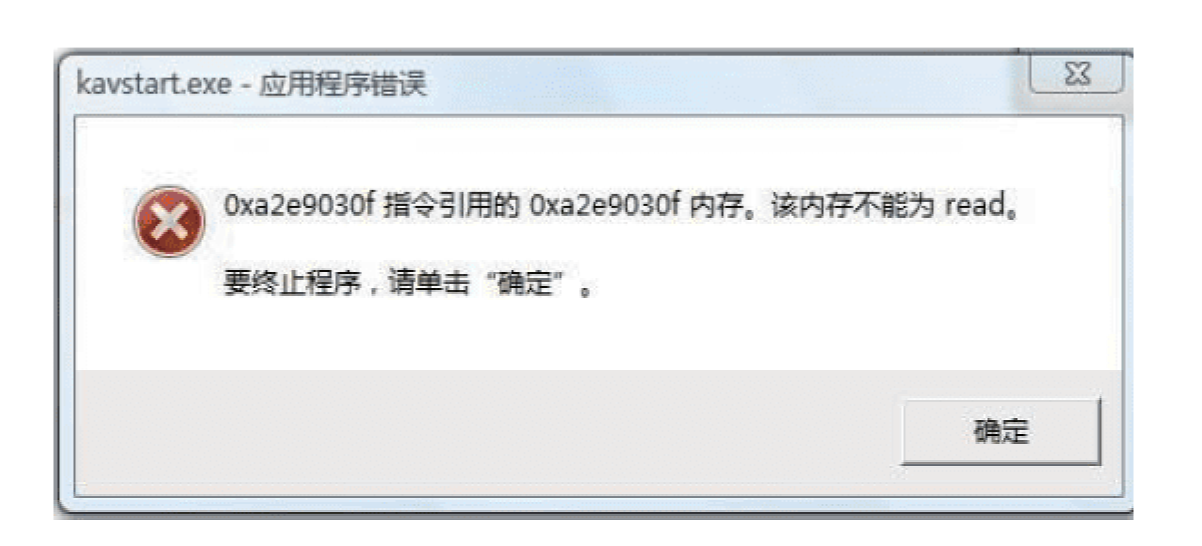
具体分析：内存出错导致系统重启的几率相对较大。除内存条与插槽接触不良外，内存本身出现质量问题也会导致系统重启。另外，把内存的CL值设置得太小也会导致内存不稳定，从而导致系统自动重启。

提示：CL值设置一定程度上反映了该内存在CPU接到读取内存数据的指令后，到正式开始读取数据所需的等待时间。



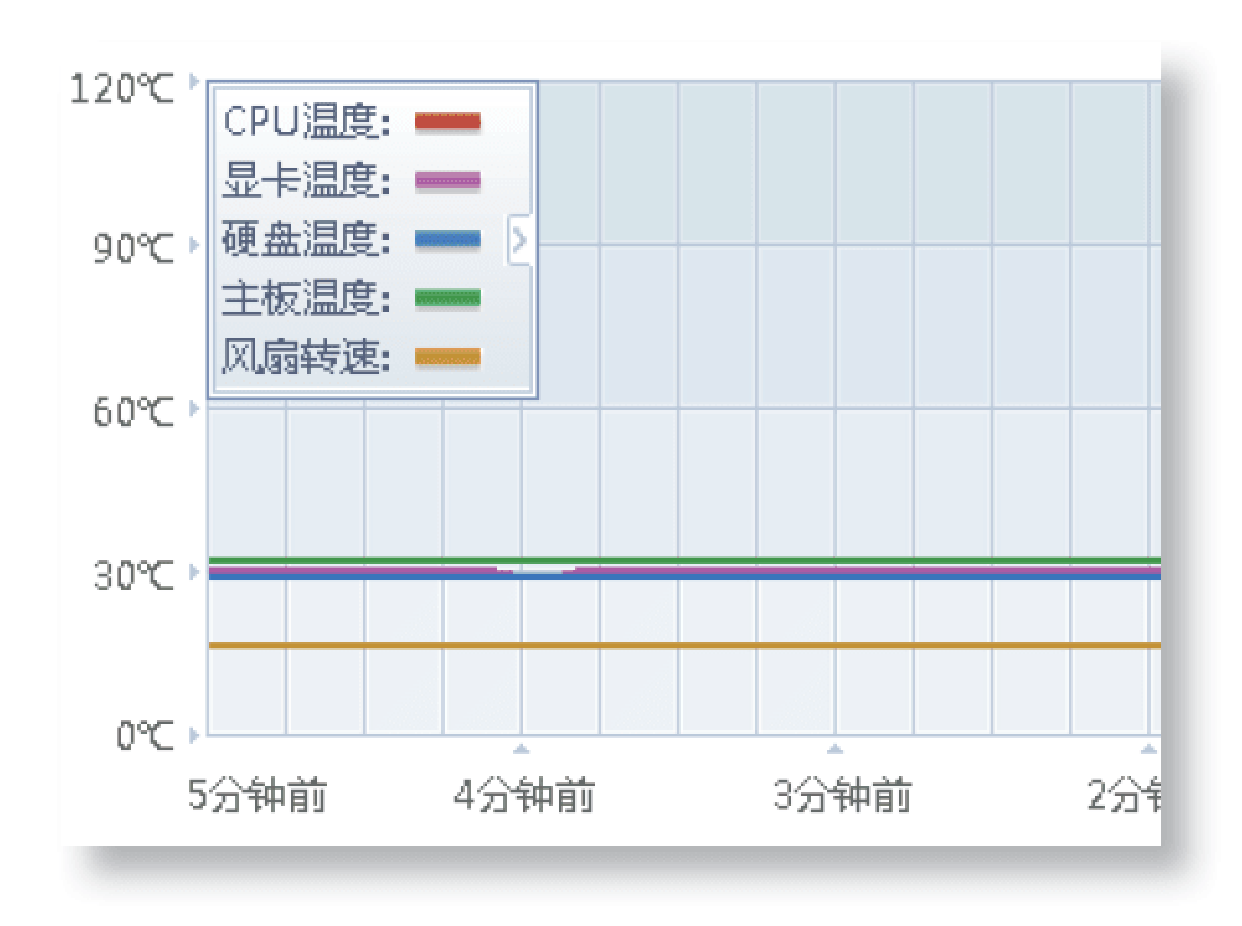
原因3：电源插座接触不良

具体分析：电源插座在使用一段时间后，弹簧片的弹性会慢慢丧失，导致插头和弹簧片之间接触不良，电阻不断变化，电流也随之起伏，系统自然会很不稳定，一旦电流达不到系统运行的最低要求，电脑就会重启。



原因4：硬件不兼容

具体分析：硬件不兼容一般指主板与内存条的不兼容，但显卡的不兼容也会导致系统不断重启的现象。



原因5：系统运行时硬件温度过高

具体分析：电脑主机箱中各种设备的连线杂乱，阻碍各硬件的正常散热；CPU风扇或电源风扇运转不正常，无法正常散热；CPU超负荷运行，产生大量热量无法排出。

3. 外界条件的影响

电脑的正常工作也会受外界条件的影响，如供电电压过低、强磁场以及灰尘过多等情况都有可能导致电脑的重启。因此，在电脑的使用过程中应注意其外界环境，并养成良好的操作习惯。



下面将对外界条件引起的电脑重启现象进行简单介绍。

原因1：电压不稳

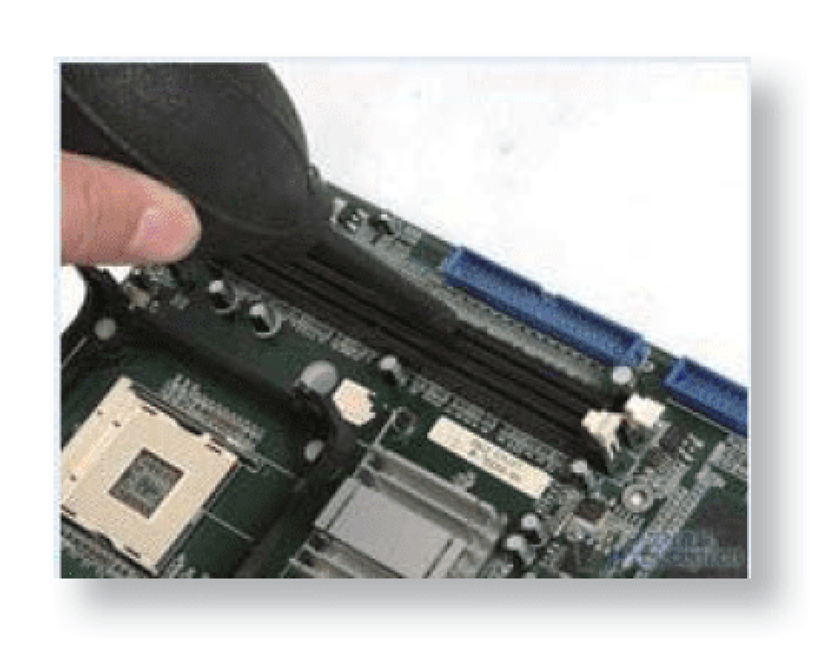
具体分析：电脑的电源工作电压一般为170V～240V，当电压低于170V时，电脑会自动重启。如果电脑和空调、冰箱等大功耗电器共用一个插线板，在其启动的时候，供给电脑的电压就会受到很大的影响，可能导致电脑重启。

原因2：强磁干扰

具体分析：机箱内部的CPU风扇、机箱风扇、显卡风扇、显卡、主板和硬盘的磁场，外部的动力线、变频空调甚至汽车等大型设备的磁场，都会干扰到电脑的正常运行。如果电脑的抗干扰性能差或屏蔽不良，就会出现电脑意外重启。

原因3：积尘太多

具体分析：电脑如果积尘太多，会引起主板上影响电脑启动的线路短路，从而导致自动重启。



11.1.2 电脑自动重启故障急救

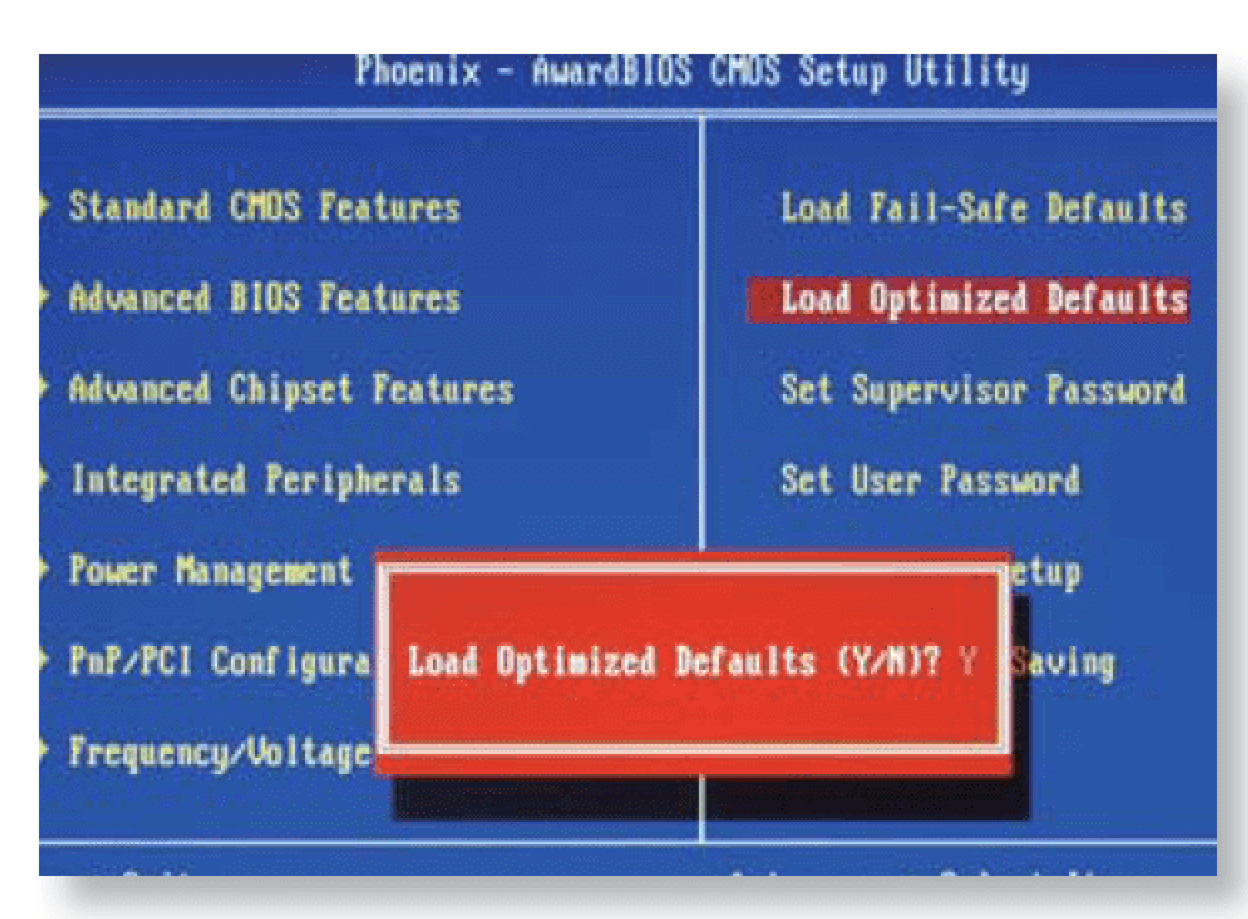
了解了电脑自动重启的原因，用户可以根据具体情况采用相应的方法进行故障排除，从而达到电脑急救的目的。



在电脑出现自动重启现象时，首先应对其原因进行排查，然后再进行相关的急救处理，下面将对常见的解决办法进行讲解。

1. BIOS设置引起的重启急救

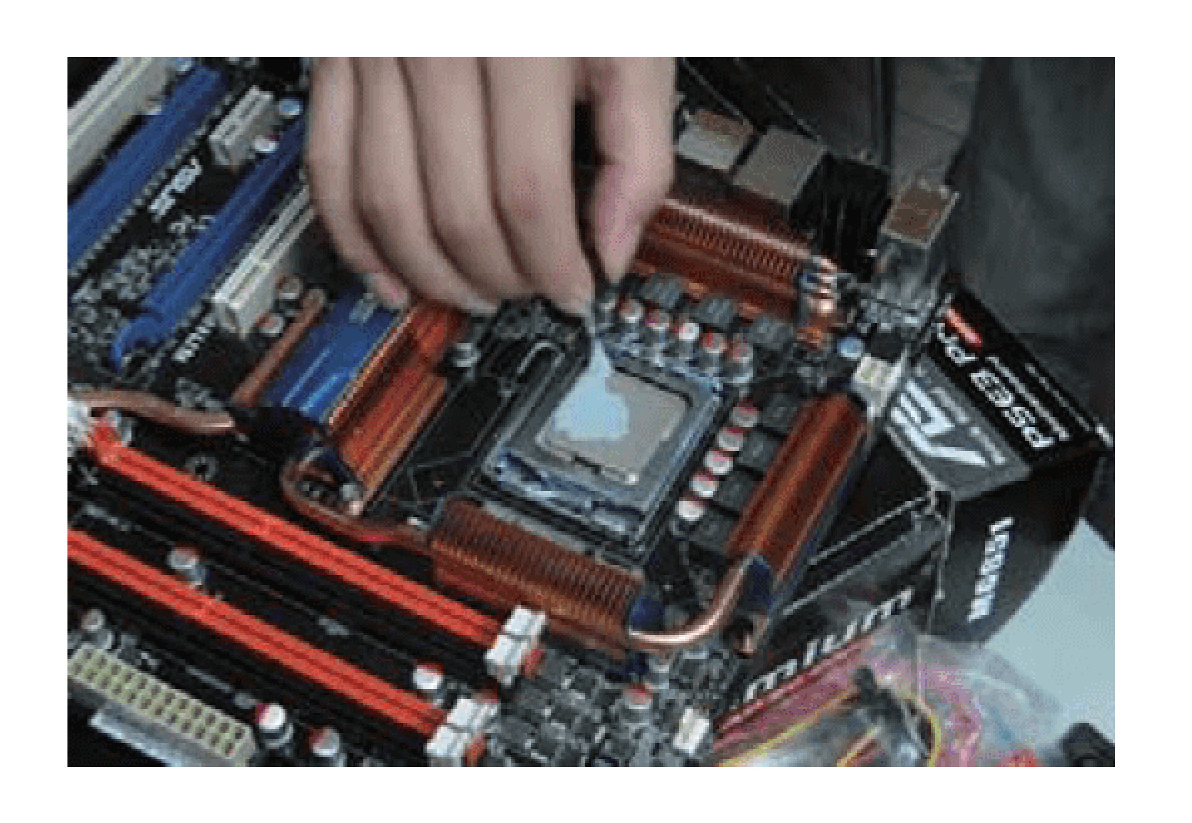
电脑自动重启有可能是BIOS的设置出现了问题，解决方法是：进入BIOS中，将其恢复默认设置；或把主板的电池拿出来，反扣放电，等5分钟再装进去。这样可以使BIOS的设置恢复默认值，解决由于BIOS的散热预设而引起的自动重启或关机现象。





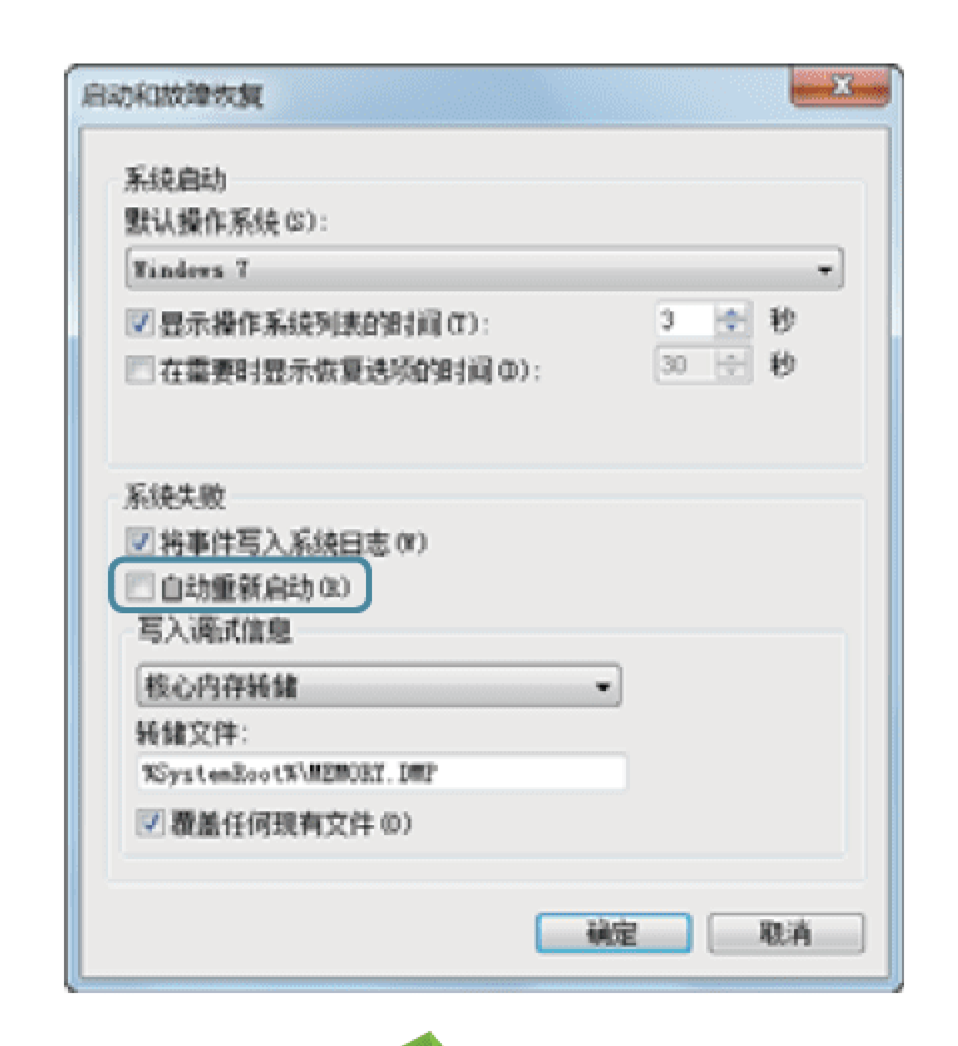
2. 病毒引起的自动重启急救

开机按F8键进入安全模式，然后使用瑞星杀毒软件查杀病毒。如果重启电脑后故障排除，则是病毒造成的重启故障。



3. 检查CPU温度

电脑的CPU温度过高可引发重启，解决方法是：将主板从机箱内取出检查或测试，接着检查CPU风扇散热片的底部硅胶是否变干，如果变干，将CPU风扇上的硅胶清理干净，然后重新涂上新的硅胶即可；最后检查CPU风扇的转动情况以及CPU的温度是否正常。



4. 取消系统默认的自动重启设置

取消系统默认自动重启设置的方法为：在“计算机”图标上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开的窗口中单击“高级系统设置”超链接，在打开对话框的“启动和故障恢复”栏中单击设置(T)...按钮，在打开的对话框中取消选中“自动重新启动”复选框，单击确定按钮即可。

教你一招

通过注册表设置禁止自动重启

在“运行”对话框中执行regedit命令，打开注册表编辑器，在其中展开HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/CrashControl选项，在其右侧窗格中双击AutoReboot选项，在打开对话框的“数值数据”文本框中将其数值设置为0，然后单击确定按钮，即可将自动重启任务取消。



5. 更换电脑电源或其他硬件设备

将电脑中的电源更换为优质的电源，可以解决由于电脑硬件过多导致电量不足和因电源质量问题带来的电压不稳的现象，从而解决电脑因电源问题而造成的自动重启现象。另外，如果内存和显卡与主板不兼容，将其更换也能解决自动重启的问题。

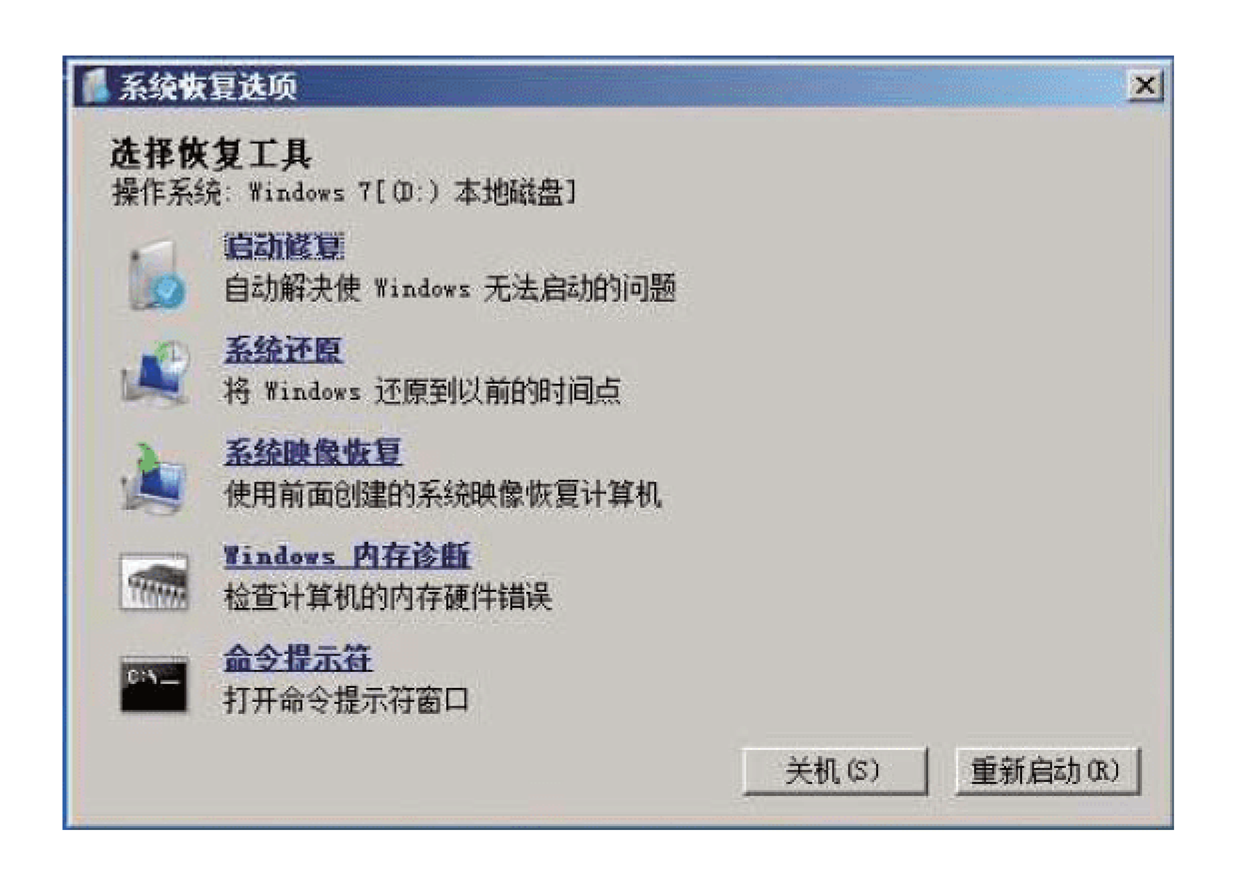
新手解惑

Q：对软件导致的电脑自动重启故障应怎样进行排除？

A：如安装应用程序或运行程序软件时电脑发生重启，则说明该重启是程序软件引起的。一般而言，将程序软件卸载重装即可解决该问题。如故障依旧，则说明软件本身有错误。

6. 修复系统文件

当电脑出现自动重启现象时，可使用安装光盘修复系统文件，以重新获取被损坏的文件，使系统能够正常运行。其方法为：将系统光盘放入光驱中，运行安装程序进入安装向导，根据向导进行操作，选择系统修复功能即可对系统文件进行扫描并修复。



跟我练习

使用学过的方法排除电脑自动重启的原因

任务1：首先使用360硬件大师检测电脑硬件的温度是否正常，如一切都正常，再使用杀毒软件进行病毒的查杀。

任务2：打开“高级系统设置”对话框，在其中查看是否启用了“自动重新启动”功能，如启动了，关闭该功能。

任务3：恢复BIOS默认设置，然后检查电脑自动重启故障是否解决。如故障依旧存在，则更换电脑电源并检查各插座是否接触良好。

11.2 电 脑 死 机

这天，娜娜正在使用电脑进行月底的销售统计，电脑突然就死机了，这可把娜娜急坏了。她不想让做了这么久的工作变成无用功，于是急急忙忙找到阿伟，想让阿伟为她保存这些资料。但是阿伟看了以后，摇摇头说：“没办法了，只有重启电脑看能不能恢复。”娜娜很失望，她苦恼地问阿伟：“怎样才能让电脑不死机或者少死机呢？”阿伟接下来就为娜娜讲解起了为什么电脑会死机。

11.2.1 电脑死机的原因

死机是指电脑在正常运行时，突然出现无法使用鼠标和键盘，电脑不再做任何反应的现象，一般只能通过重启电脑来解决。死机的原因，通常可分为硬件故障和软件故障两方面。





由于软件和硬件故障引起电脑死机的情况有很多种，下面分别进行介绍。

1. 软件方面

下面将对一些常见的由软件引起的死机现象进行简单介绍。

- 执行了含有错误代码的软件或程序。
- 同时运行多个程序引起操作混乱，电脑无法响应。
- 电脑病毒破坏，导致系统文件出现错误或丢失。
- 硬盘空间不足，导致系统数据周转空间不足。
- 硬盘的坏道过多，在运行程序时死机。
- 系统BIOS设置不当。

2. 硬件方面

下面将对一些常见的由硬件引起的死机现象进行简单介绍。

- 主板上元件接触不良或老化，主板芯片不稳定或出现问题。
- 系统中的接口卡与主板接触不良，内存工作不稳定。
- 部分存储地址损坏。
- 主机电源功率不足，CPU超频使用或温度过高。

教你一招

防止电脑死机的措施

打开杀毒软件的实时监控功能，并定期升级病毒库；为电脑配置稳定的电源；正确地安装和卸载软件，尽量安装正版的软件；在运行大型软件时尽量减少同时运行的程序数量。

11.2.2 电脑死机故障急救

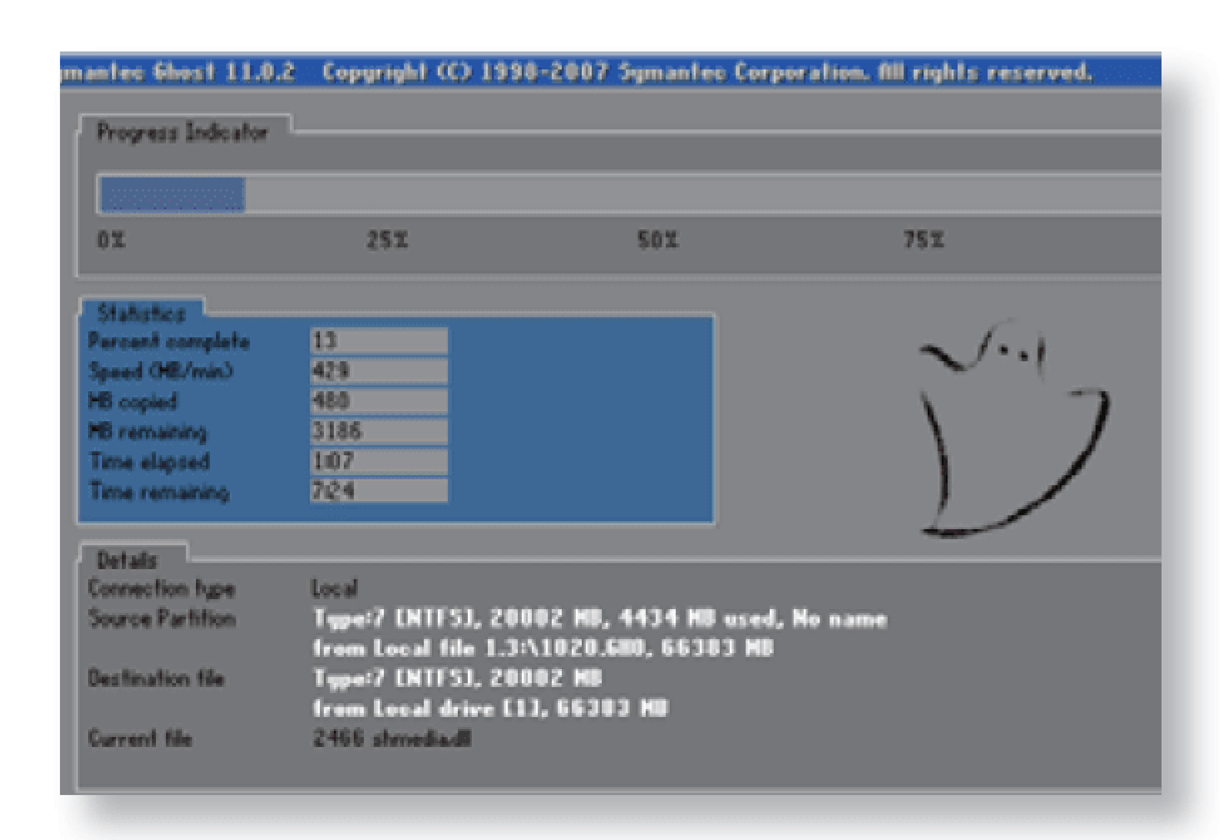
在学习了死机故障的原因后，对电脑死机的一般原因有了简单的了解。电脑出现死机现象常常是由于电脑资源的不足或灰尘所引起的。下面将介绍常见的死机故障急救方法。

1. 死机故障急救的一般过程

在使用电脑时，不慎删除Windows目录下的某个文件、感染了病毒或磁盘碎片过多都会造成电脑死机现象。

知识点拨

下面将对死机故障的一般处理方法进行讲解。



还原系统：在电脑中使用安装的MaxDOS软件将系统的备份文件进行还原，排除系统问题。

提示：要使用MaxDOS软件，需在电脑中先安装它。

查杀病毒：使用360杀毒软件进行病毒的查杀，排除由于病毒引起的电脑死机故障。



教你一招

选择杀毒软件和杀毒方法

用户还可以选择瑞星、江民和金山杀毒软件进行病毒的查杀，并且可以开机按F8键进入安全模式下进行病毒的查杀。

磁盘碎片整理：运行磁盘碎片整理程序，进行磁盘碎片的整理。电脑死机也可能是由于用户的反复复制、删除文件，导致硬盘上碎块过多而引起的。





教你一招

磁盘碎片整理的方法

选择“开始”/“所有程序”/“附件”/“系统工具”/“磁盘碎片整理程序”命令，打开“磁盘碎片整理”对话框，在其“当前状态”列表框中选择要整理的磁盘，然后单击磁盘碎片整理(D)按钮，即可对选择的磁盘进行碎片整理。

2. 灰尘引起的死机故障急救

电脑在运行程序时经常死机，天气潮湿时死机现象更为频繁，这表明电脑可能是由于灰尘引起的死机。下面将对因灰尘引起的死机现象急救方法进行讲解。

打开机箱外壳，如发现主板上堆积了很多灰尘，并且灰尘比较潮，说明数据线漏电。天气潮湿时，漏电情况会更严重，因此死机也会更频繁。清除机箱内的灰尘后，死机故障即可得到解决。



跟我练习

检测电脑死机的原因

首先使用360杀毒软件对电脑进行病毒查杀，排除因病毒造成的电脑死机现象；然后使用系统自带的磁盘碎片整理程序对磁盘碎片进行整理，并使用Ghost恢复系统；最后再检查电脑硬件方面的原因。通过上述步骤推测出死机故障的产生原因。

11.3 电脑蓝屏

阿伟告诉娜娜，蓝屏也是在使用电脑过程中经常遇到的故障，它经常困扰着不懂电脑的用户。于是娜娜问道：“电脑蓝屏与其他故障的主要不同点在哪里？”阿伟回答道：“电脑蓝屏指的是Windows操作系统无法从某个系统错误中恢复过来时所显示的屏幕图像。”知道了这些，娜娜开始要求阿伟为她讲解电脑蓝屏方面的知识。

11.3.1 电脑蓝屏的原因

Windows之所以要蓝屏，是因为它不知道该错误是否能被隔离出来，从而不伤害系统的其他程序与数据。如果该异常来源于更深层的问题，则允许系统继续运行会导致更多的异常。Windows意识到这样做的风险太大了，因此，为了程序和数据的安全与完整，为了将损失在第一时间内降至最低，于是采取了蓝屏保护措施。



电脑蓝屏可从软件和硬件两方面来分析，下面将分别对其进行讲解。

1. 软件方面

从软件方面来看，电脑蓝屏与电脑自动重启和死机类似，主要是由于病毒、BIOS设置以及误删除了系统文件等方面的原因造成的。

A problem has been detected and windows has been shut down to prevent damag
to your computer.

The problem seems to be caused by the following file: nv4_disp.dll

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xE584CA08,0x00000000,0xBD0C87A3,0x00000001)

*** nv4_disp.dll - Address BD0C87A3 base at BD012000, DateStamp 4a2462f8

原因1：病毒

具体分析：如果用户的电脑感染了病毒，当病毒将系统中的相关文件删除后，会造成电脑的频繁死机或直接蓝屏。为防止这种情况发生，应在电脑中安装杀毒软件。

原因2：BIOS设置不当

具体分析：当BIOS设置不当，即硬盘、内存在BIOS中的相关选项设置不当时，会导致电脑蓝屏现象。



提示：恢复BIOS默认设置有时也会导致蓝屏，这是因为系统认为更换了硬件，此时需重新安装操作系统才能解决蓝屏现象。



原因3：动态链接库文件的丢失

具体分析：后缀为.dll的文件是系统盘内的重要文件，从性质上来讲属于共享类文件。也就是说，一个DLL文件在运行时会有多个软件调用它，如果由于软件运行错误导致了DLL文件的丢失，则也会造成电脑蓝屏。



2. 硬件方面

电脑硬件方面的原因主要是指内存松动、硬盘出现坏道或软硬件不兼容等情况，它们也可能会导致电脑蓝屏。



下面将对引起电脑蓝屏的硬件原因进行讲解。

- **软硬件不兼容导致蓝屏：** 新技术、新硬件的发展很快，如安装了新的硬件后电脑出现蓝屏，则可能是因为主板的BIOS或驱动程序太旧，以致不能很好地支持硬件。
- **内存的接触和兼容问题：** 有些组装机在玩游戏的过程中或在安装了某种软件后出现蓝屏，主要是因为内存条不兼容或者是内存条松动。
- **硬盘坏道或坏扇区：** 硬盘出现坏道或坏扇区时，会影响到操作系统的正常运行，如硬盘的坏道或坏扇区正好是操作系统文件的存储位置，则电脑可能会出现蓝屏现象。

11.3.2 蓝屏故障急救

一般情况下，蓝屏都是在硬件驱动或新加硬件并安装驱动后，出现冲突或不兼容的情况，这时可重启电脑，按F8键，使用Windows操作系统提供的“最后一次正确配置”来解决此问题，但对于一些特殊情况则要仔细进行分析原因才能找到解决的办法。



下面将对一些常见的蓝屏代码以及处理方法进行简单介绍。

1. 0x0000007B

0x0000007B：INACESSIBLE_BOOT_DEVICE，Windows在启动过程中无法访问系统分区或启动卷。一般发生在更换主板后第一次启动时，主要是因为新主板和旧主板的IDE控制器使用了不同芯片组造成的，有时也可能是病毒或硬盘损伤造成的。用安装光盘启动电脑，然后执行修复安装即可解决问题。对于病毒，则可进入电脑安全模式，使用杀毒软件进行查杀。

A problem has been detected and windows has
to your computer.

If this is the first time you've seen this s
restart your computer. If this screen appear
these steps:

Check for viruses on your computer. Remove a
hard drives or hard drive controllers. Check
to make sure it is properly configured and t
Run CHKDSK /F to check for hard drive corrup
restart your computer.

Technical information:

*** STOP: 0x0000007B (0x80D86B58,0xC0000034,

提示：出现此种代码还可能是硬盘本身存在问题，处理办法是将其安装到其他电脑中，然后使用“chkdsk /r”命令来检查并修复磁盘错误。另外，BIOS设置问题也可能造成此种现象，只要将BIOS设置为IDE模式即可。

2. 0x00000079

0x00000079：MISMATCHED-HAL，硬件抽象层与内核或机器类型不匹配（通常发生在单处理器和多处理器配置文件混合在同一系统的情况下）。要解决本错误，可使用命令控制台替换电脑中错误的系统文件。

A problem has been detected and windows has been shut down to
to your computer.

MISMATCHED_HAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure that any new hardware or software is proper
If this is a new installation, ask your hardware or software m
for any windows updates you might need.

If problems continue, disable or remove any newly installed ha
or software. Disable BIOS memory options such as caching or sh
If you need to use Safe Mode to remove or disable components,
your computer, press F8 to select Advanced Startup Options, an
select Safe Mode.

Technical information:

*** STOP: 0x00000079 (0xF3438BFC,0x647453A2,0x56A439C8,0xF9948

*** fastfat.sys - Address 0xF569C091 base at 0x6432C2AD, Dates

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error
restart your computer. If this screen appears again,
these steps:

Check to make sure any new hardware or software is pr
If this is a new installation, ask your hardware or s
for any windows updates you might need.

If problems continue, disable or remove any newly ins
or software. Disable BIOS memory options such as cach
If you need to use Safe Mode to remove or disable com
your computer, press F8 to select Advanced Startup Op
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFFADF774391E4,0x0000000000

3. 0x00000050

0x00000050：PAGE_FAULT_IN_NONPAGED+AREA，内存（包括物理内存、二级缓存和显存）、不兼容的软件（主要是远程控制和杀毒软件）、损坏的NTFS卷以及有问题的硬件。如电脑中安装有MaxDOS，可在命令模式下直接删除C盘的页面文件。



教你一招

怎样区分电脑死机和蓝屏故障？

电脑死机和蓝屏的不同之处在于，蓝屏时屏幕上会出现故障提示信息，用户可以根据这些提示信息找到解决的办法，而死机则没有任何提示。

```
A problem has been detected and Windows has been shut down to prevent dam
to your computer.

PFN_LIST_CORRUPT

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:
*** STOP: 0x0000004e (0x00000099, 0x00000000, 0x00000000, 0x00000000)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

4. 0x0000004e

0x0000004e：PFN_LIST_CORRUPT，这是内存存在问题时最典型的提示。这个现象在启动电脑时就可以查看到，通常是启动不了电脑，画面提示内存有问题是否要继续。其原因是物理内存遭到损坏或者内存与其他硬件不兼容。这时通过更换内存即可解决。

```
A problem has been detected and windows has been shut down to
prevent damage to your computer.

IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly
If this is a new installation, ask your hardware or software
manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed h
or software. Disable BIOS memory options such as caching or s
If you need to use Safe Mode to remove or disable components,
your computer, press F8 to select Advanced Startup Options,
select Safe Mode.

Technical information:

*** STOP: 0x0000000A (0x00000000,0x00000002,0x00000001,0x808
```

5. 0x0000000A

0x0000000A：IRQL_NOT_LESS_OR_EQUAL，某些软件或硬件与Windows不兼容。如遇到0x0000000A错误，建议尝试以“最后一次正确的配置”方式启动Windows，并检查最近有没有安装或升级过任何系统更新、硬件设备的驱动程序、BIOS及应用软件等。如有，将其卸载、恢复到之前可以稳定运行的版本即可。

新手解惑

Q：对于一些没见过的蓝屏代码应该怎样处理？

A：访问Windows官方网站，在知识库中输入这些蓝屏错误代码，即可查询到其含义以及处理方法。

跟我练习



首先使用电脑的“最后一次正确的配置”选择进入操作系统，再重启电脑进入安全模式，使用杀毒软件查杀电脑中的病毒，然后更换电脑内存，如问题依旧，则修复或重新安装操作系统。

11.4 IE浏览器故障急救

尽管前面已经讲过很多关于IE浏览器方面的知识，但阿伟还是决定再给娜娜讲解一些关于它的问题。知道阿伟的想法后，娜娜好奇地问：“阿伟，你还有哪些关于IE浏览器的知识呢，前面不是都已经讲过了吗？”阿伟回答道：“这次主要给你讲解一些IE浏览器的常见故障以及在遇到这些故障时该如何去解决。”

11.4.1 IE浏览器故障分析

使用IE浏览器的过程中，可能会遇到一些情况导致IE浏览器运行出现故障而无法使用，这时用户将无法进行网页的浏览及资料的查询。



IE浏览器出现故障的原因有系统文件被破坏、IE浏览器的设置不当和恶意程序破坏等几种，下面将分别进行介绍。

- **系统文件被破坏：** 操作系统运行过程中，无法保证其系统文件的安全性。IE浏览器作为Windows系统的核心组件之一，也不例外。当IE浏览器运行所需要的系统文件被破坏后，其功能就无法实现，甚至出现运行不正常的情况。
- **IE浏览器的设置不当：** 如果用户在使用过程中对IE浏览器进行了错误设置，也会导致IE浏览器无法正常打开网页。
- **恶意程序破坏：** 网络信息包罗万象，有的网页中加入了恶意程序，这些程序利用IE浏览器的漏洞，会修改IE浏览器的主页、标题栏和搜索引擎等设置，而且还会修改系统的启动项（使系统在启动时加载恶意程序，从而导致系统故障）。





Q：怎样防范恶意程序破坏浏览器？

A：上网时打开病毒防火墙，防止网页中有恶意程序运行；定期升级IE浏览器，及时安装安全补丁；对于陌生的网站要确认无误后再打开访问；网上下载的文件先进行病毒扫描，然后再打开；安装IE浏览器保护软件，利用软件修复IE浏览器出现的故障。

11.4.2 IE浏览器故障急救实例

用户在遇到IE浏览器故障时，只要采取相应的措施，就可以将IE浏览器恢复正常。下面将介绍一些常见的IE浏览器故障急救方法。

1. IE浏览器无法打开新窗口

使用IE浏览器打开新的网页时，IE浏览器没有任何反应，出现这种情况可能是由于IE新建窗口模块被破坏，重新注册相应模块即可。



下面将重新注册IE新建窗口模块，其具体操作如下。

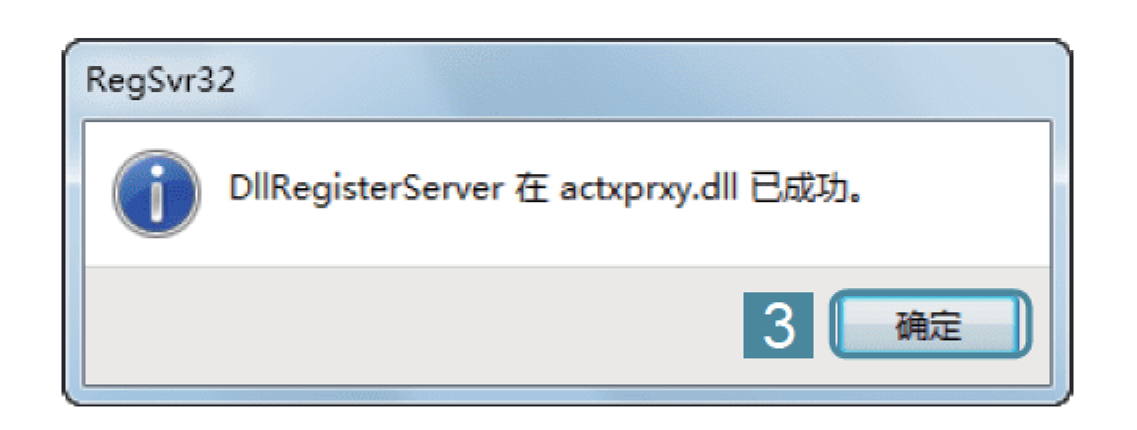


第1步：重新注册actxprxy.dll模块

选择“开始”/“运行”命令，打开“运行”对话框，在该对话框的“打开”文本框中输入“regsvr32 actxprxy.dll”，然后单击确定按钮。

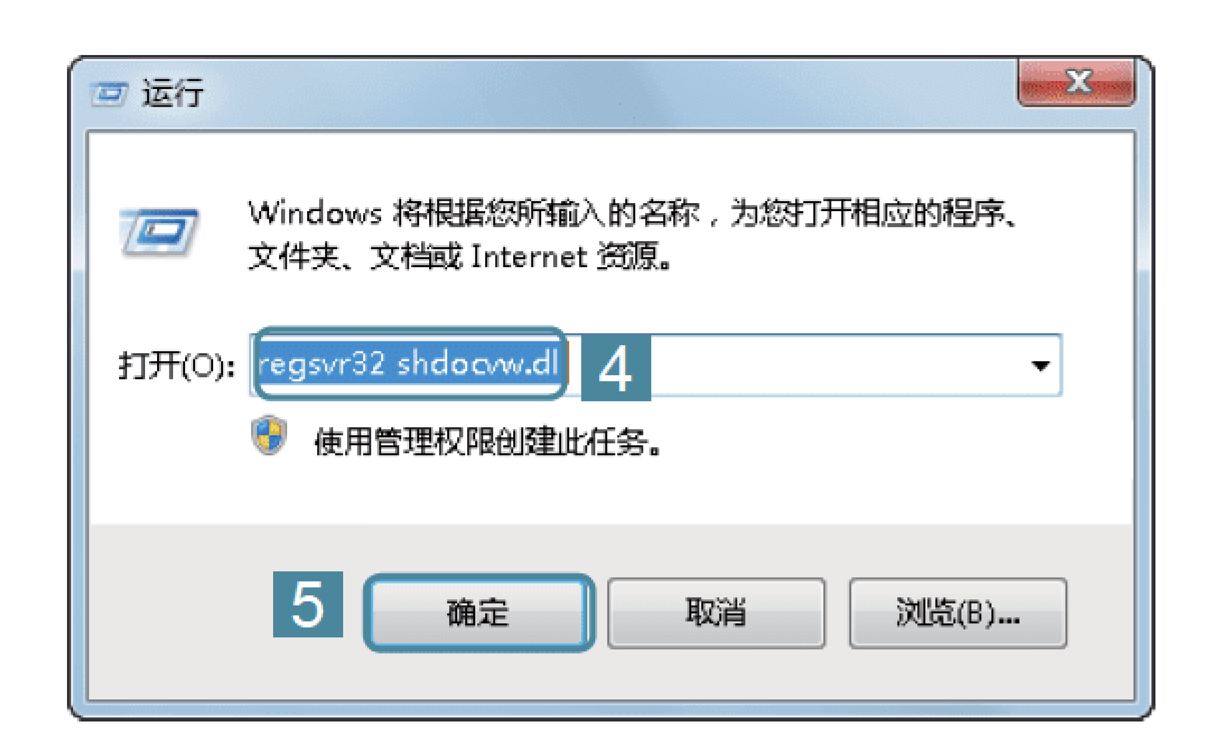
第2步：完成注册

在打开的对话框中将提示regsvr32 actxprxy.dll注册成功，然后单击确定按钮。



第3步：注册shdocvw.dll模块

继续在“运行”对话框的“打开”文本框中输入“regsvr32 shdocvw.dll”命令，单击确定按钮，然后重新启动电脑。



教你一招

如进行了以上操作还不能解决问题，则还可以进行哪些操作？

如果问题依旧，可以使用相同的方法将mshtml.dll、urlmon.dll、msjava.dll、browseui.dll、oleaut32.dll和shell32.dll也重新进行注册。

2. IE浏览器运行出错

IE浏览器也是程序，有时运行出错是难免的。在IE浏览器运行出错后，将弹出错误报告对话框，可以给Microsoft公司发送IE运行错误的报告。



这里以IE 8.0为例来讲解关闭错误报告的方法，其具体操作如下。

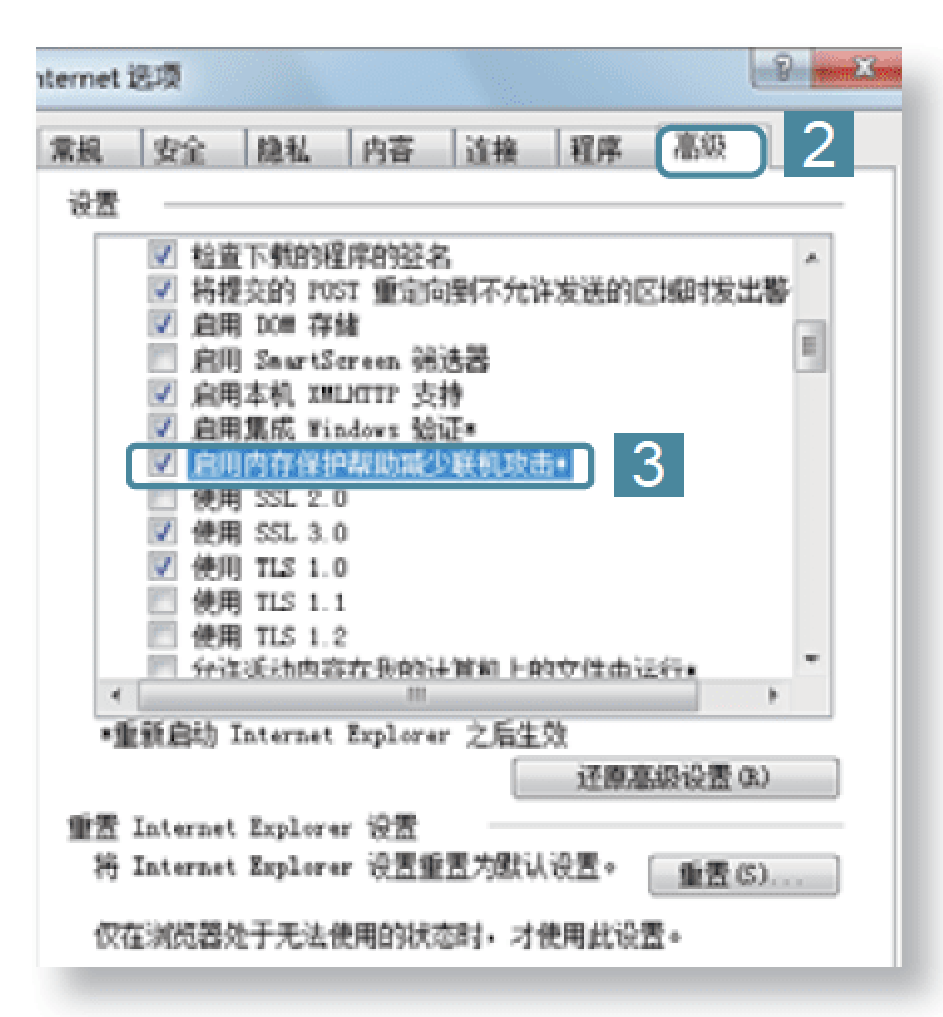


第1步：打开“Internet 选项”对话框

选择“开始”/“控制面板”命令，在打开的窗口中单击“Internet 选项”超链接，打开“Internet 选项”对话框。

第2步：设置高级选项

在打开的对话框中选择“高级”选项卡，在其中的“设置”列表框中选中“启用内存保护帮助减少联机攻击”复选框，然后单击确定按钮应用设置。







Q：IE 8.0 出现错误报告的原因是什么？

A：主要原因是程序设计不够严谨，问题较多，并且占用较多的系统资源。另外，虽然提升了部分安全控件，在理论上提升了安全性，可没有提升任何安全系数，反而让一些正常的网站访问不正常，从而出现错误。

3. 可登录QQ但无法打开网页

用户使用ADSL上网时，经常会遇到电脑能登录QQ但却无法浏览网页的现象。这时，用户需仔细检查和分析原因。



下面将对其原因和处理方法进行简单介绍。

- **感染了病毒所致：** 如确认是电脑感染了病毒，就需要使用杀毒软件对系统进行全面的扫描。注意，杀毒软件的病毒库应该是最新的，否则不能查杀到最新的病毒。
- **DNS服务解析出错：** DNS即域名服务器，它可以将域名转换成电脑能够识别的IP地址，如新浪（www.sina.com.cn）对应的IP地址是218.30.66.63。如果DNS服务器出错，则无法进行域名解析，也就不能上网。如拨号后不能正确获取DNS地址，则需手动设置DNS地址。
- **系统文件丢失导致IE不能正常启动：** 如果用户的操作系统运行不稳定，经常出现死机、重启和非法关机等现象，就会造成系统文件丢失。此时，可用sfc命令来修复丢失的系统文件。

4. IE浏览器被恶意修改

IE浏览器被恶意修改后，其默认主页将呈灰色显示，无法进行设置，其标题栏也被修改了。此时，可使用超级兔子修复被修改的IE浏览器。



下面将使用超级兔子2012扫描IE浏览器相关选项并进行修复，其具体操作如下。



第1步：检测系统中的问题

在电脑中安装了超级兔子2012后，双击其快捷方式图标启动程序。在其主界面中，系统将自动进行检测并显示检测结果。系统检测完毕后，单击“系统中有1个恶意网址”选项右侧的“查看并修复”超链接，即可查看检测到的恶意网址。



第2步：清除恶意网址

在打开的界面中将显示恶意网址，选中“恶意网址”前的复选框，然后单击 立即修复 按钮，系统将对该恶意网址进行清除。

提示：单击 开始扫描 按钮再次进行扫描，直到不能检测出恶意程序为止。

第3步：修复IE

选择“系统防护”选项卡，在其中选择“IE修复”选项，系统将进行扫描并显示扫描结果，单击 立即修复 按钮，将对扫描的结果进行修复，完成后在对应的选项后将显示“修复完毕”。



新手解惑

Q：超级兔子的主要功能有哪些？

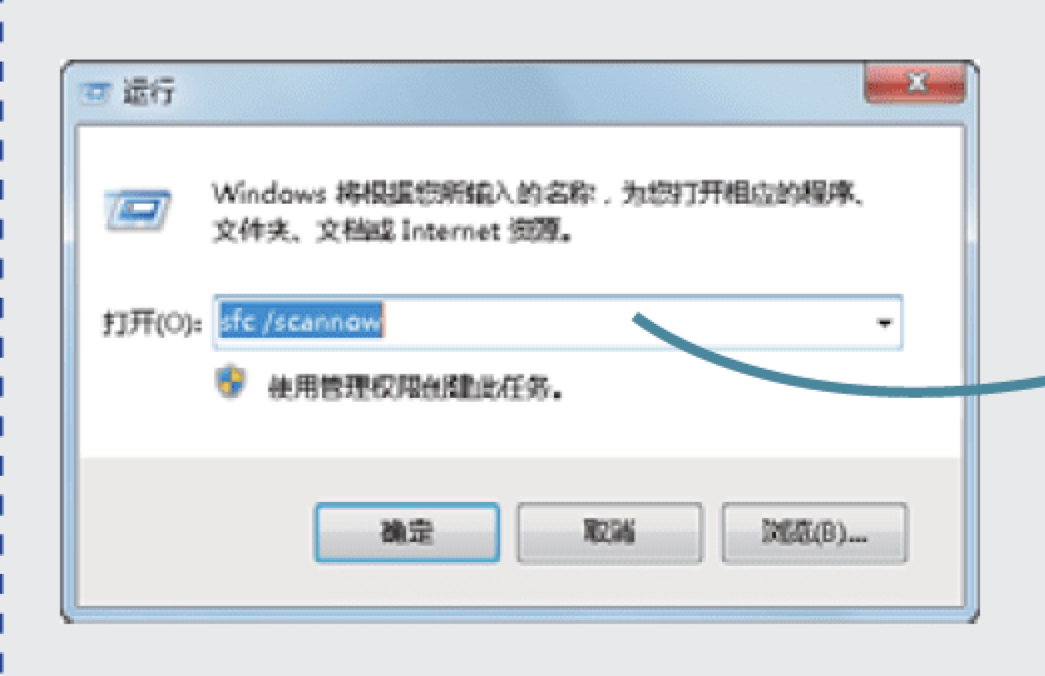
A：超级兔子的主要功能是优化系统，同时还可以对系统进行个性化设置。

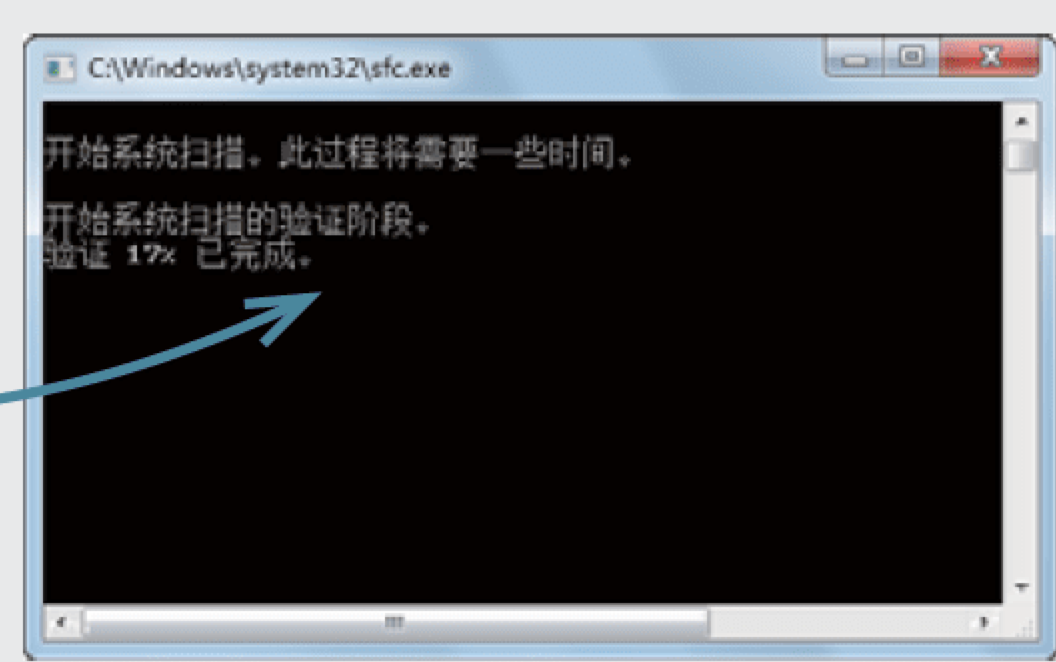


教你一招

如何验证系统文件的完整性？

选择“开始”/“运行”命令，打开“运行”对话框，在“打开”文本框中输入“sfc /scannow”命令后单击 确定 按钮，在打开的窗口中将显示Windows正在验证系统文件的完整性。





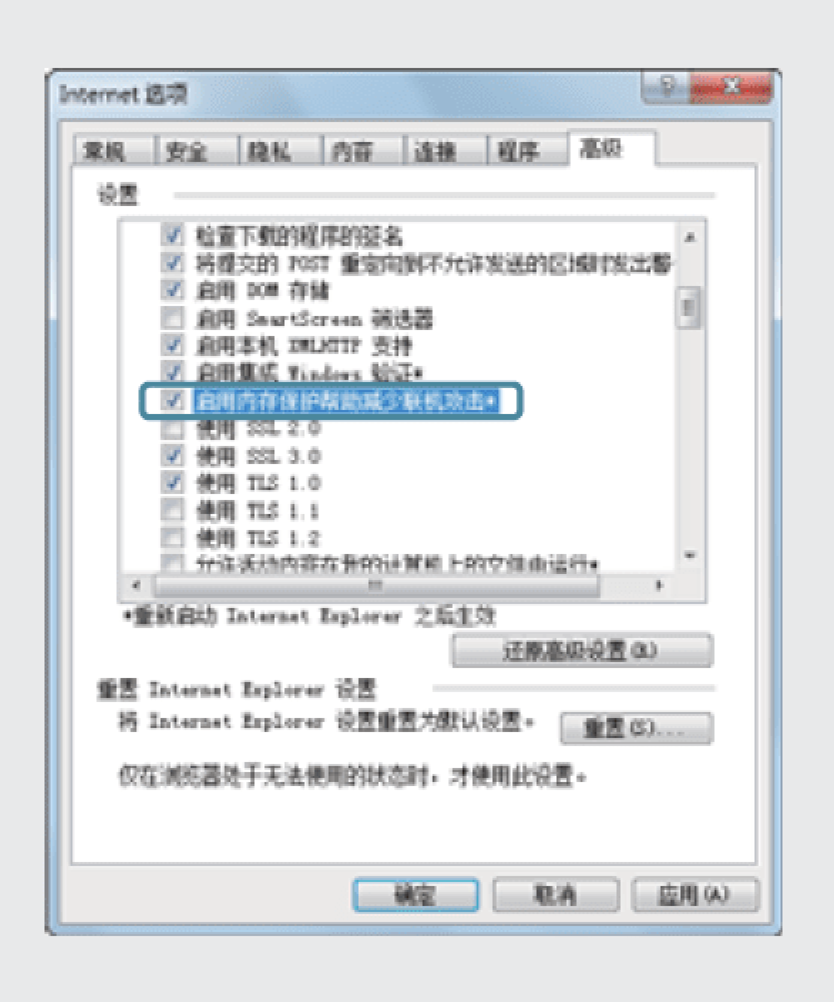
跟我练习

为了避免IE浏览器发生故障，娜娜决定按阿伟讲解的知识对自己的电脑重新进行设置

任务1：打开“Internet 选项”对话框，在其中的“高级”选项卡中选中“启用内存保护帮助减少联机攻击”复选框。

任务2：打开“运行”对话框，重新注册新建窗口的相关模块。

任务3：在电脑中安装超级兔子2012，并使用其进行系统的相关扫描，修复IE浏览器被恶意篡改的选项。





11.5　办公软件故障急救

娜娜听了阿伟的讲解后，对于电脑的常见故障有了更清晰的认识。但是今天，娜娜突然想到如果自己天天使用的办公软件也出现了故障，自己一定会束手无策。于是娜娜又赶紧向阿伟请教有关常用办公软件故障急救方面的知识。

11.5.1　Word故障急救

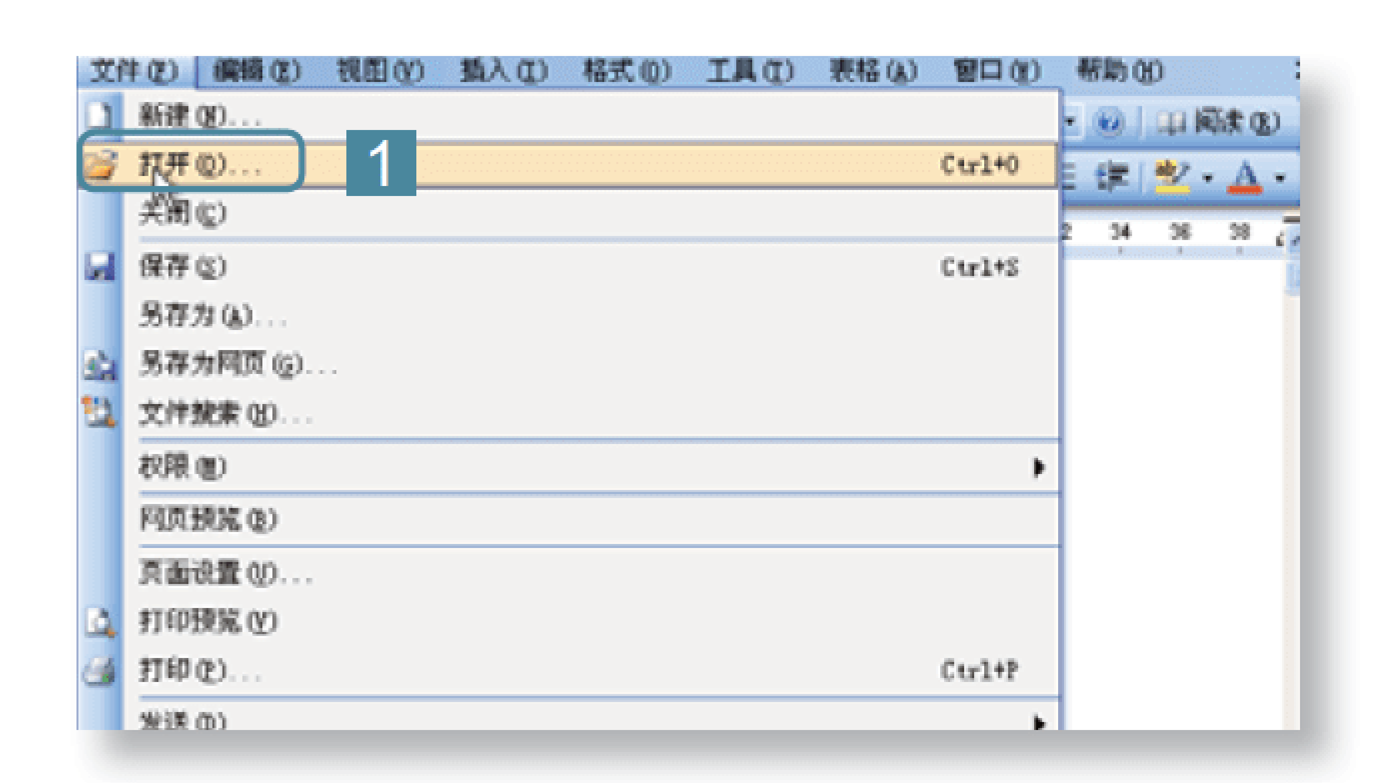
Word中常见的故障有文档损坏、打印出错和右键菜单丢失。要正常使用Word进行各类文档处理，必须熟练地解决这些故障。

1. Word文档损坏

当出现Word 2003文档损坏时，如电脑中只安装了Word 2003，则可手动进行修复。



下面将使用Word 2003的修复功能手动修复文档，其具体操作如下。



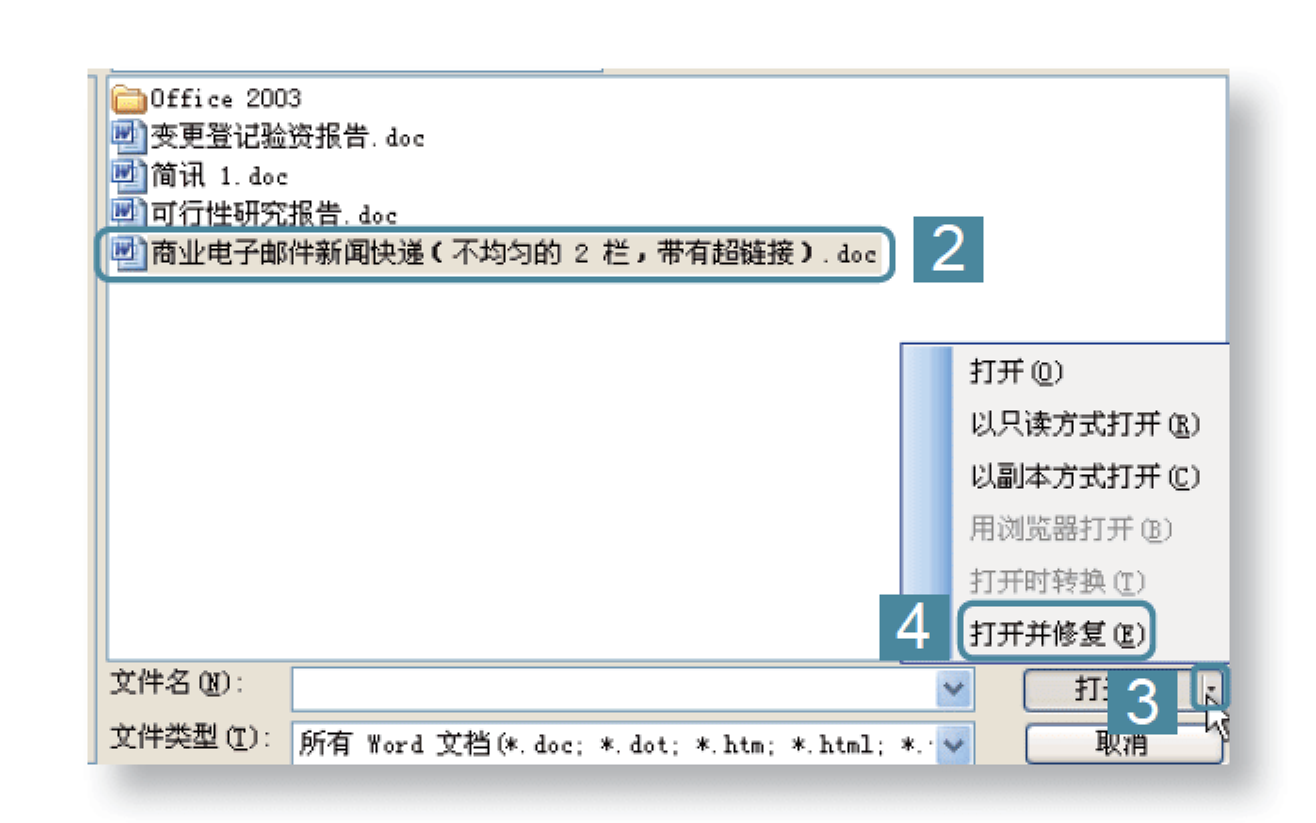
第1步：选择“打开”命令

启动Word 2003，在Word窗口中选择“文件”/“打开”命令。

提示：在Word 2007和Word 2010中打开文档时可以自动修复损坏的文件。

第2步：修复文档

在“打开”对话框中选择需要修复的文档。单击 打开(O) 按钮右侧的下拉按钮，在弹出的菜单中选择“打开并修复”命令，即可修复损坏的文档。



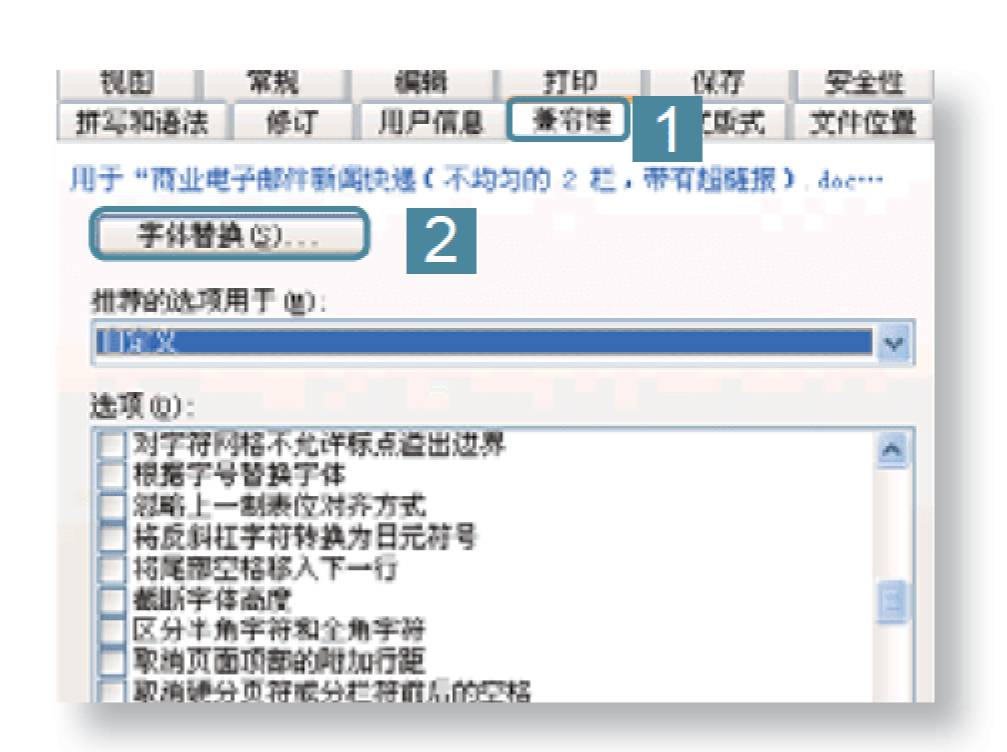


2. 打印Word文档出错

在Word中打印文档时，有时系统会出现“文档字体错误”提示，这可能是由于电脑或打印机无法识别该文档中的某些字体。此时，只要安装这些字体或者将这些出现错误的字体更改为电脑中已经安装的字体即可。



下面将使用替换字体的方法将电脑或打印机无法识别的字体替换成其他字体，其具体操作如下。

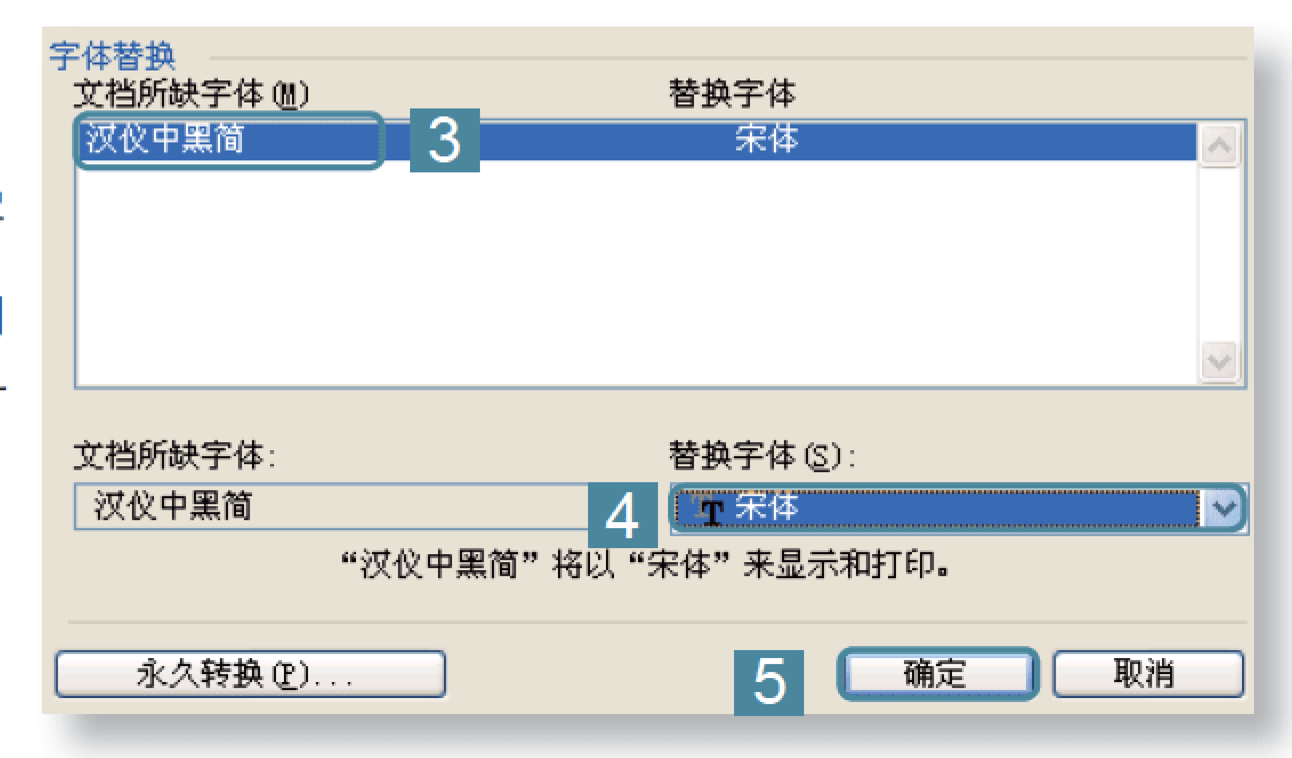


第1步：打开“字体替换”对话框

打开打印出错的文档，在其窗口中选择“工具”/“选项”命令，打开“选项”对话框，选择“兼容性”选项卡，然后单击 字体替换(S)... 按钮，打开“字体替换”对话框。

第2步：替换字体

选择需要替换的字体，在“替换字体”下拉列表框中选择需要替换为的字体，然后单击 确定 按钮，即可进行替换。



3. Word 2010中右键菜单丢失

有的用户电脑上原来安装的是Office 2007，当卸载后重新安装Office 2010时，会发现安装完后其他功能都正常，但单击鼠标右键时没有快捷菜单。这可能是因为电脑中安装的Babylon在Word中添加了插件而引起的，可在Word窗口中选择相应的选项进行处理。



下面将简单介绍加载右键菜单的方法，其具体操作如下。

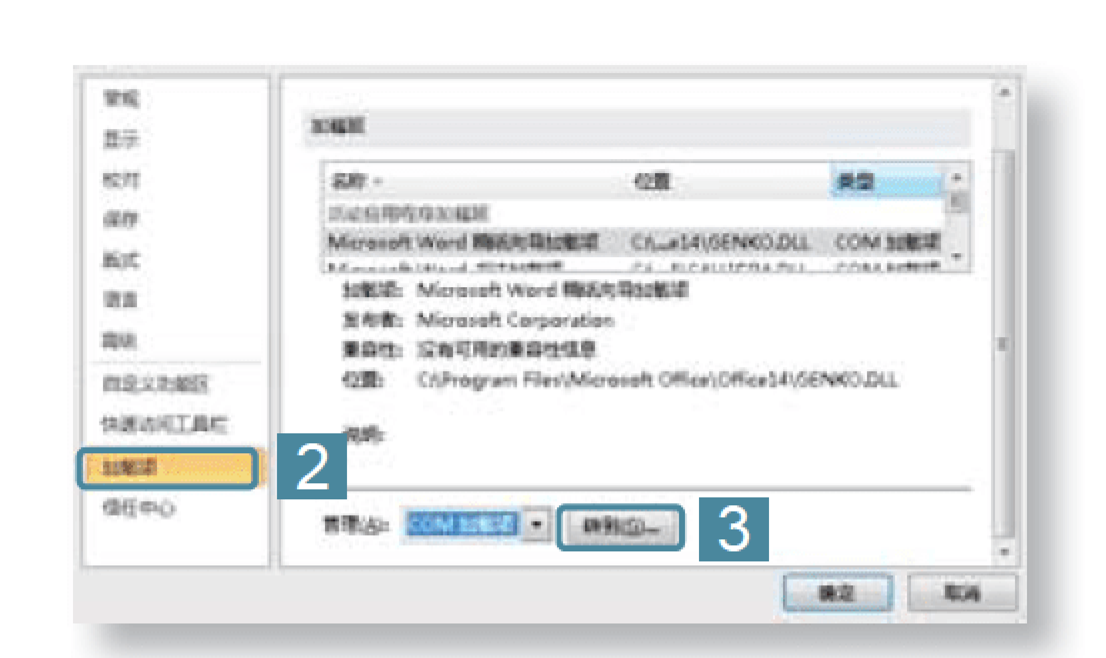
第1步：打开“Word 选项”对话框

启动Word程序，在其中选择“文件”/“选项”命令，打开“Word 选项”对话框。



第2步：打开加载项对话框

在打开的对话框中选择左侧窗格中的“加载项”选项卡，在右侧窗格中单击 转到(G)... 按钮。



第3步：选择相应的加载项

在打开对话框的“可用加载项”列表框中选择需要的加载项，然后依次单击 确定 按钮即可。

11.5.2 Excel故障急救

用户在使用Excel时，有时会遇到出现错误提示、出现无效的页面以及弹出错误信息等问题。要处理这些问题，首先应了解其故障原因。

1. Excel出现错误提示

遇到Excel错误提示时，可根据其提示内容进行相应的处理。



以下是常见的Excel提示信息的含义和解决方法。



- #DIV/O!：公式生成的数字过大或过小。这时只需修改公式，使其结果在有效数字范围之内即可解决。如果函数中使用了不能接受的参数，修改函数中的参数类型即可解决。
- #NULL：使用了不正确的单元格引用或区域运算符。这时应首先检查单元格引用是否正确，再检查区域运算符是否正确。如要对两个区域求和，在公式中引用这两个区域时，必须使用逗号分开。
- #VALUE!：在公式或函数中使用了错误的数据类型。将公式或函数中的运算符或参数修改正确，并确认公式引用的单元格中包含有效的数值。
- #N/A：在输入的函数或公式中没有可用数值。如果某个单元格暂时没有数值，可在该单元格中输入“#N/A”，公式在引用这些单元格时就不会进行数值计算。
- #REF!：如果删除了由其他公式引用的单元格，可能引起这种错误，这时需重新更改公式。将移动单元格粘贴到了由其他公式引用的单元格中，删除或粘贴单元格后，执行撤销操作即可恢复工作表中的单元格。
- #NUM!：公式产生的数字太大或太小，或使用了迭代计算的工作表函数 但该函数不能产生有效的结果，或在需要数字参数的函数中使用了不能接受的参数。可以通过修改公式使其结果在有效数字范围内，为工作表函数使用不同的初始值以及修改函数的参数类型来解决。
- #####!：当Excel中单元格所含的数字、日期或时间比单元格宽，或单元格的日期时间公式产生了一个负值时，就会出现该错误。如果是单元格所含的数据比单元格宽，可以通过拖动列表之间的宽度来增加列宽；如果公式正确，可将单元格的格式改为非日期和时间型来显示；如果使用的是1900年的日期系统，Excel中的日期和时间必须为正值。

教你一招

出现其他错误代码时的处理方式

在Excel 2010中，还有其他一些错误信息提示，由于篇幅有限，这里不一一讲解。读者如遇到其他错误信息提示，可通过Excel帮助查找该问题的解决方法。

2. Excel出现无效页面错误

用户在使用Excel分析较大的数据量时，有时会出现“无效页面”的错误提示，选择确定后会关闭应用程序。



要解决该问题，应通过以下方法。

- **判断问题的原因：**首先进行病毒查杀，如果没有发现病毒，可以用Excel打开其他数据文件。如果一切正常，说明Excel本身没有问题，很可能只是该数据文件有错误。
- **修改数据文件：**使用SQL Server数据库软件导入该数据文件，对比导入的文件与原SQL Server文件格式的异同，将不同的格式修改后再导出，然后用Excel重新打开。

教你一招

办公软件的其他错误原因

除此之外，办公软件在使用过程中可能遇到的问题还有很多。例如，打开相关的办公文件后某些功能不能使用，这可能是由于该文件设置了控件，而自己的系统设置了不自动运行造成的。另外，一些新建的办公文档不能打开，大多数情况下是由于这些文档是由更高版本的办公软件创建的，低版本的办公软件自然无法打开。

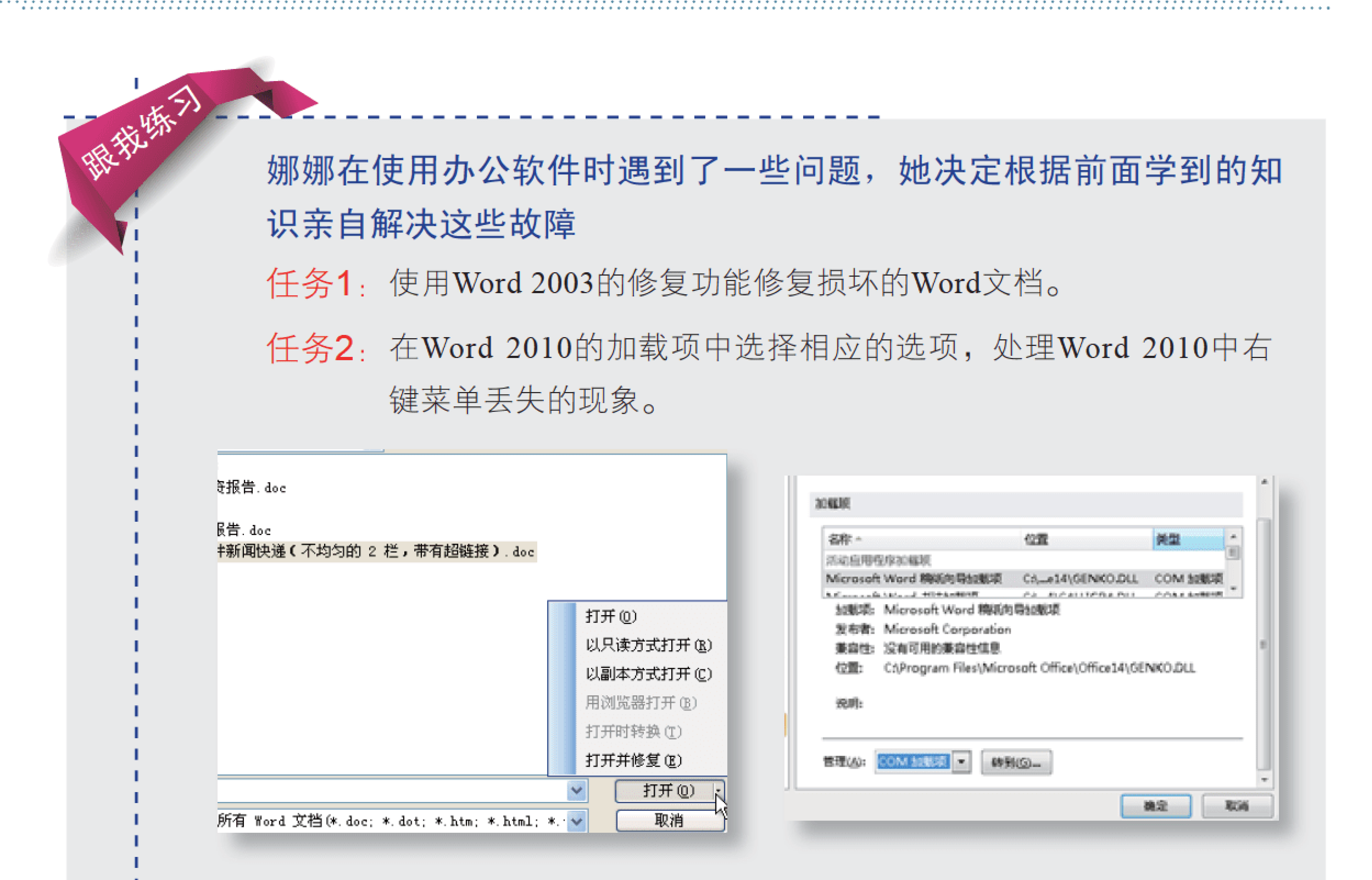
11.5.3　安装Office时出错

在Windows操作系统上安装Office 2007软件的过程中，系统有时会提示无法更新一个或多个受保护的Windows文件。出现这种问题可能是电脑中“C:\ProgramFiles\CommonFiles\Microsoft Shared\WebServerExtensions\40\Bin”路径下缺少Fp4autl.dll、Fpencode.dll和Fp4awel.dll这3个文件。可从安装光盘中找到这些文件，将其复制到Bin目录下，即可解决这个问题。如果没有系统安装光盘，也可以从安装了相同操作系统的其他电脑上复制这3个文件。

新手解惑

Q：可以在一台电脑上安装几个版本的Office软件吗？

A：可以。很多软件都可以多个版本共存。安装过程中，当提示已存在其他版本的软件时，选择自定义安装，而不选择覆盖安装就可以将多个版本的软件安装在一台电脑中。



娜娜在使用办公软件时遇到了一些问题，她决定根据前面学到的知识亲自解决这些故障

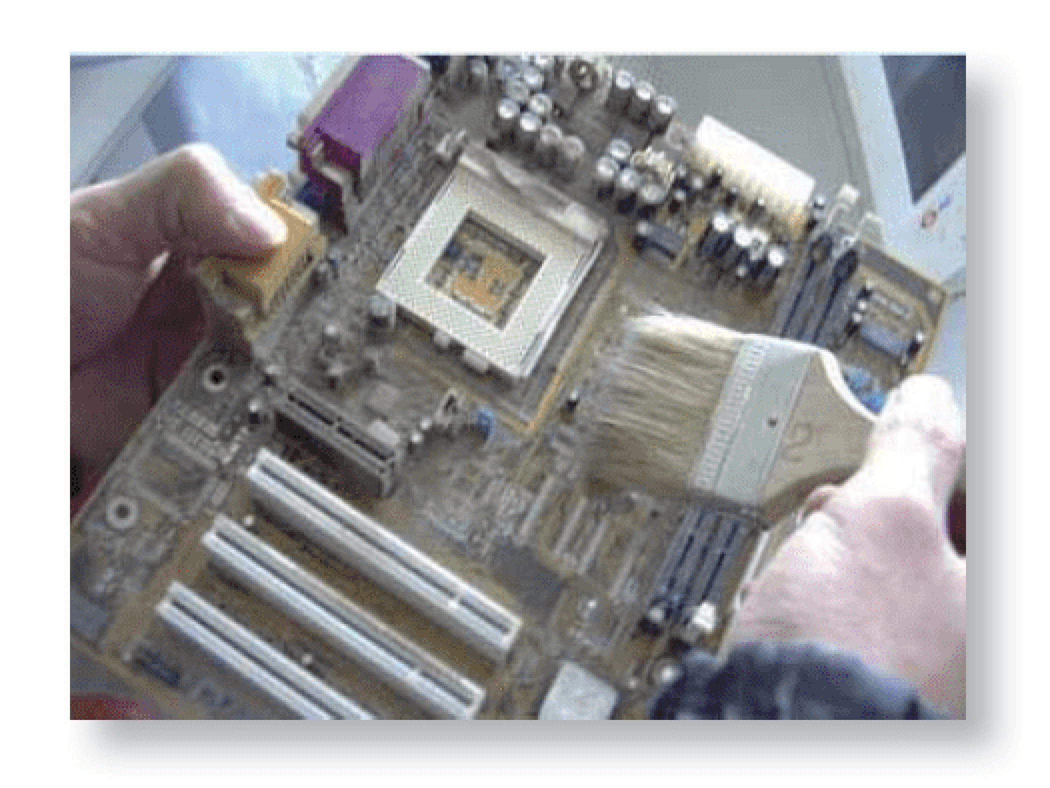
任务1：使用Word 2003的修复功能修复损坏的Word文档。

任务2：在Word 2010的加载项中选择相应的选项，处理Word 2010中右键菜单丢失的现象。

11.6 更进一步——故障轻松恢复

阿伟为娜娜讲解了这么多，对于电脑常见故障的处理，娜娜也学了很多。在实际的应用中，娜娜已经能快速地解决很多故障。阿伟感觉娜娜这段时间的学习很认真，于是想给她多讲一些电脑故障的快速处理技巧，让她多学些知识。

第1招 电脑开机时突然黑屏



黑屏一般是由于CPU、内存和显卡等出现损坏或与主板接触不良而引起的。最常见的原因是机箱内部由于长时间没有清理，积有许多尘土，导致了各个部件之间产生接触不良。拆下各部件并用毛刷清洁机箱，然后重新组装各部件即可排除故障。

第2招 IE浏览器提示出错并关闭网页



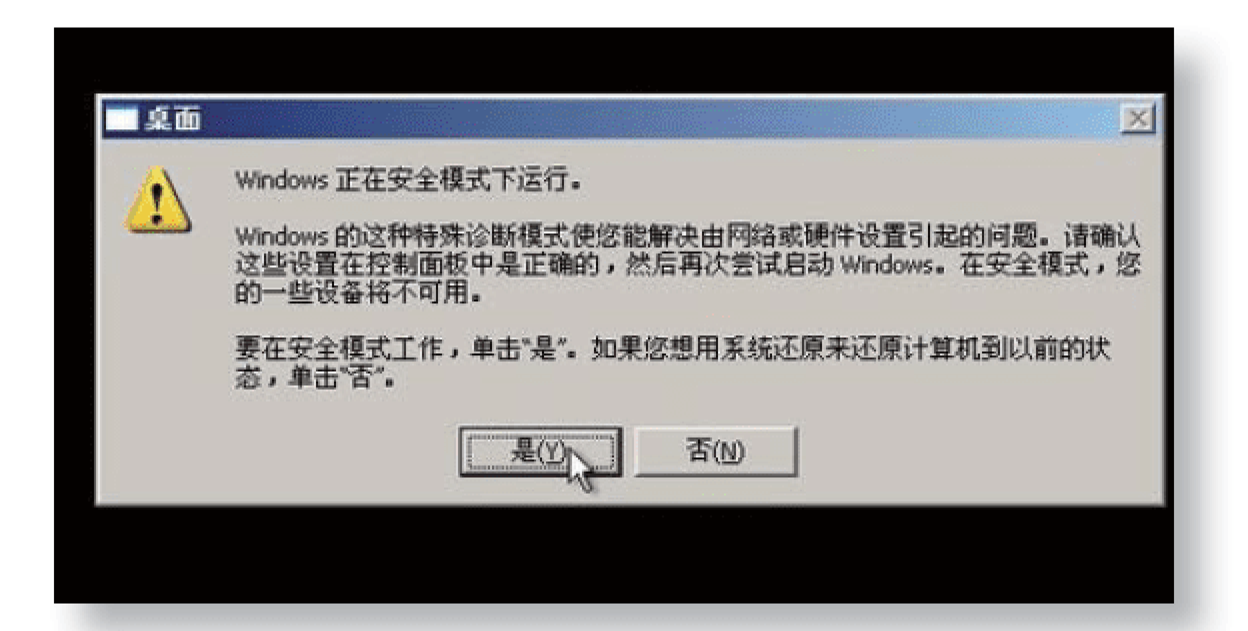
出现这种情况，可能是由于内存资源占用过多、IE安全级别设置与浏览的网站不匹配、与其他软件发生冲突、浏览的网站本身含有错误代码等原因造成的。可通过如下方法解决：

①关闭过多的IE窗口，减少内存占用，建议IE窗口打开的数量不要超过5个。

②降低IE安全级别，打开“Internet 选项”对话框，选择“安全”选项卡，单击“默认级别”按钮，拖动滑块降低默认的安全级别。

③将IE升级到最新版本。

第3招 Windows 7开机后自动进入安全模式

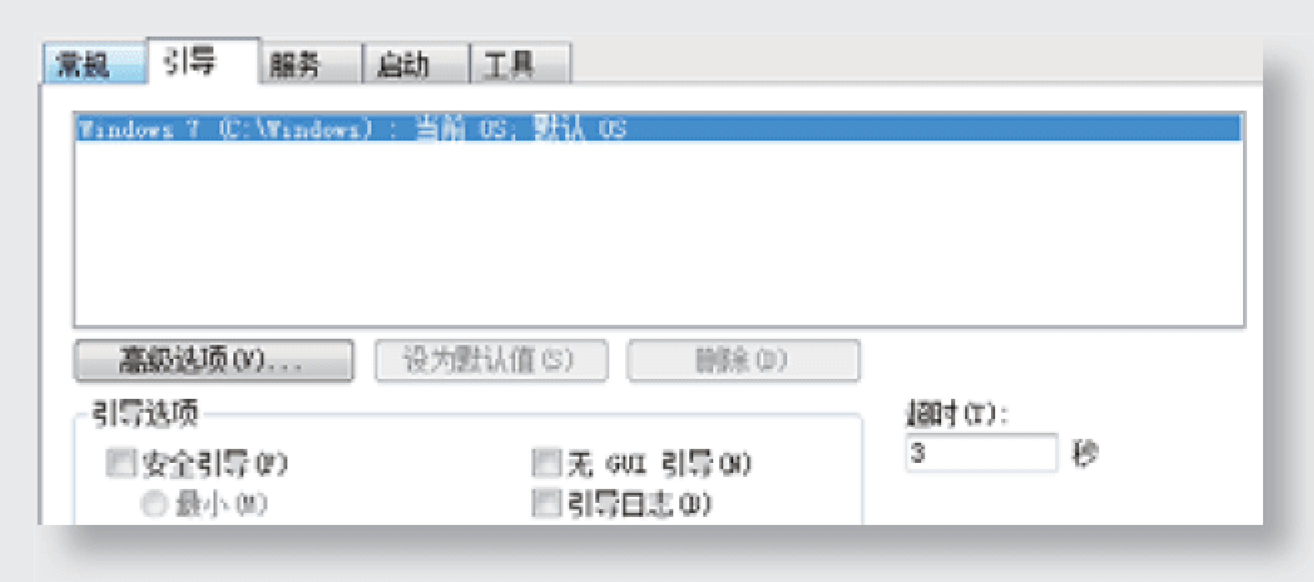


如果电脑在开机后经常自动进入安全模式，重装系统后故障依旧，则可能是由于主板与内存条不兼容或内存工作不稳定引起的。可尝试在BIOS设置中降低内存读取速度或更换内存。

教你一招

检查启动项设置，取消开机进入安全模式

打开“运行”对话框，在其中的文本框中输入“msconfig”，单击 确定 按钮，在打开的对话框中选择“引导”选项卡，在其中取消选中“安全引导”复选框，单击 确定 按钮即可。





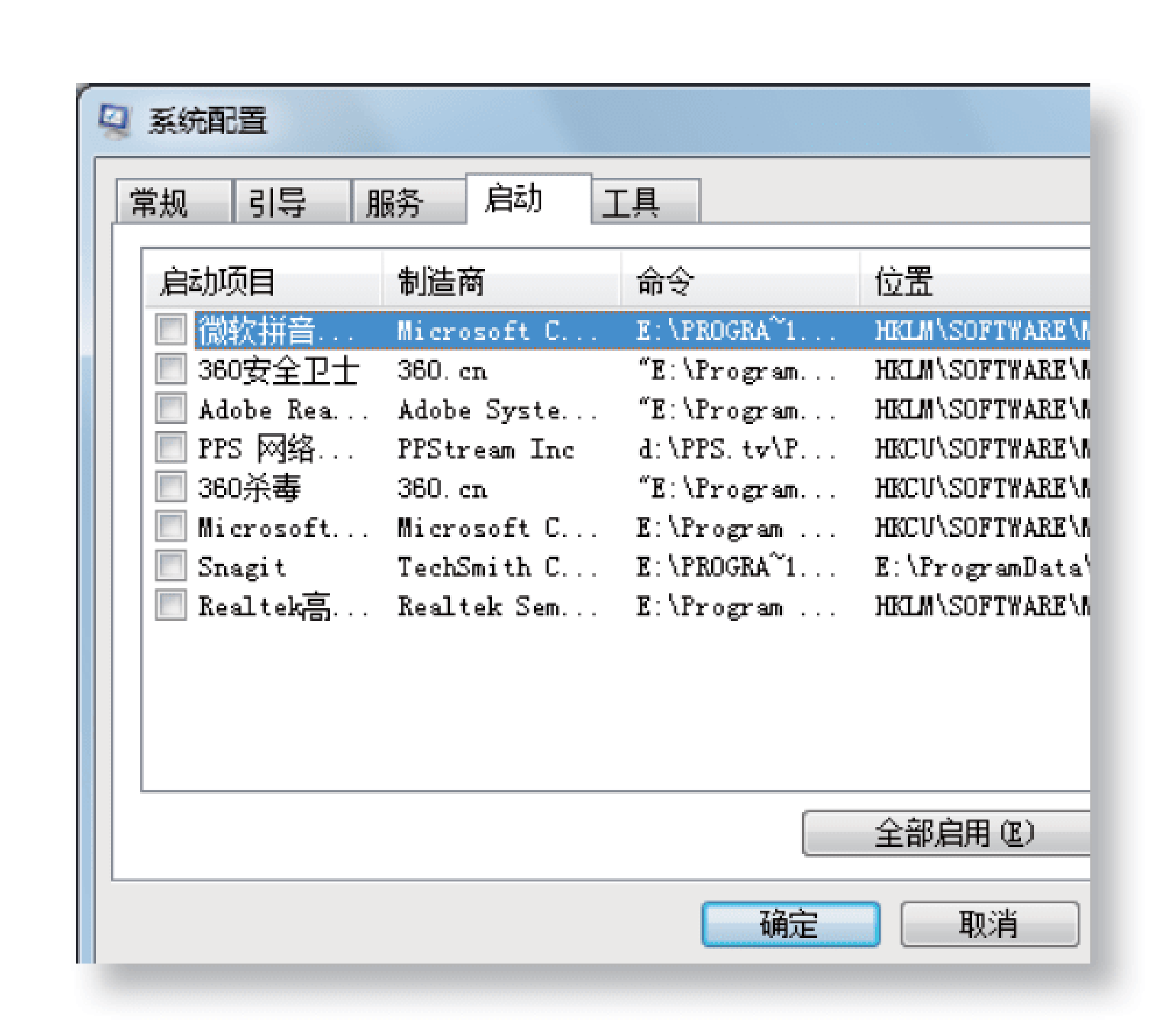
第4招 进行磁盘整理时反复重新开始

在进行磁盘整理时，有时会遇到系统在整理到 3% ～ 10%后反复重新开始整理的情况。这种故障可能是因为磁盘整理程序受到了屏幕保护程序、杀毒软件或电源管理程序的影响，其解决方法如下：

①在“运行”对话框中执行msconfig命令，打开“系统配置”对话框。

②在打开的对话框中选择“启动”选项卡，在其列表框中取消选中所有选项前的复选框。

③单击 确定 按钮即可。



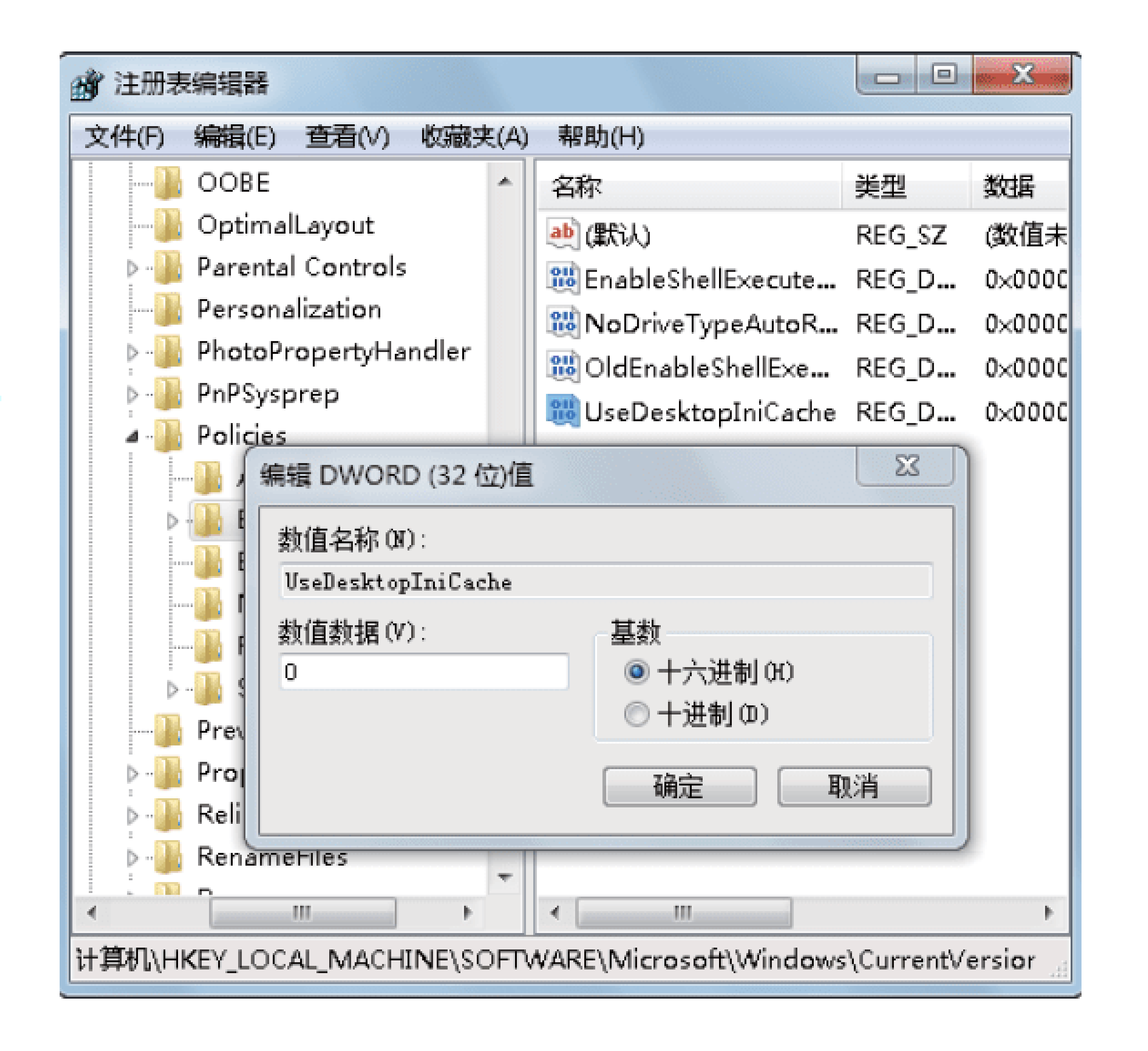
第5招 安装某些补丁时Explorer.exe出错

在Windows系统下，当安装一些补丁时，Explorer.exe会提示“遇到错误，需要关闭”，这可能是由于当前系统安装的某些补丁发生了冲突造成的。其解决方法如下：

①运行regedit命令，展开HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer选项。

②在该选项的右侧窗格中双击UseDesktopIniCache选项，在打开的对话框中将其值修改为0，然后单击 确定 按钮。

③安装更新的补丁，重启电脑后，再将UseDesktopIniCache的值改为1。



第6招 无法彻底删除Windows操作系统中的某些软件



某些软件在使用自带的卸载程序进行卸载后，在控制面板的“添加/删除程序”对话框中仍然可以看到该软件存在。这是因为这些软件不完善，卸载程序不能将其在注册表中的信息完全清除。解决方法如下：在注册表中展开HKEY_LOCAL_MADHINE/Software/Microsoft/Windows/Current Version/Uninstall选项，在其中选择相应选项删除即可。

11.7 活 学 活 用

（1）总结电脑自动重启、死机以及蓝屏的原因，对比影响其相同和不同的因素，然后再分析故障处理方法。

（2）使用杀毒软件对电脑进行病毒查杀，将BIOS恢复默认设置。

（3）使用超级兔子扫描并修复IE浏览器的异常，然后设置Internet安全选项，防止IE浏览器出现故障。

后记：提点学习建议

在创作本书时，虽然我们已尽可能设身处地为您着想，希望能解决您遇到的所有与电脑安全与急救相关的问题，但我们仍不能保证面面俱到。如果你想学到更多的知识，或学习过程中遇到了困惑，除了可以联系我们之外，还可以通过下面的渠道来解决。

善用网络资源： 网络中包含了电脑安全与急救的具体问题解决方法、电子图书、视频教程，读者没必要一一记住各个网站的网址，善用搜索引擎如百度（http://www.baidu.com），在解决问题的过程中补充自己的知识量。

加强实际操作： 学习的目的在于应用，所以在学习理论知识之余，一定要上机操作书中讲的，及通过其他渠道学习的内容，这样才能在操作的过程中巩固知识，也不容易忘记。

勤于思考和总结： 放下书本，静心想一下，其实保护电脑的方法有很多相通之处，在电脑中操作的地方也无外乎几处——控制面板、注册表、组策略，发现与总结它们的异同，这样在遇到没有学习过的问题时，说不定您一样可以轻松搞定。

多看相关资讯： 电脑的安全是一个永远不会停止的话题，其外部面临的威胁和攻击手段，随时都在更新、发生变化。只有不断通过杂志、网络学习新的资讯，才可能真正解决遇到的问题。

加强交流与沟通： 多与朋友交流学习和实战心得，如果现实中精通电脑安全与急救的朋友比较少，可以在网络中寻找，现在网上有很多这类的论坛供大家交流，也有QQ群，在查找QQ群里输入查找关键字“电脑安全”，就会出现所有的群列表，然后加入进去即可。